ISSN 0956-9979 MAY 1998

VIRUS BULLETIN

THE INTERNATIONAL PUBLICATION ON COMPUTER VIRUS PREVENTION, RECOGNITION AND REMOVAL

IN THIS ISSUE:

• **Catch-22?** This issue's *Windows 95* comparative review attracted twenty-two anti-virus products from all over the world. Compare old favourites with several new faces, starting on p.10.

• **Winning team:** *IBM's* Sarah Gordon and Frédéric Perriot clear up the potential confusion about the hoax-like nature of the RedTeam virus. Sort it out for yourself on p.6.

• **Under the microscope:** American *Intel Corporation* and Russian *Kaspersky Lab* put their current product releases up for scrutiny in our standalone reviews, starting on p.22.

CONTENTS

GUEST EDITORIAL

What You Don't See, Can't Hurt

As the complexity of computing deepens, functionality changes offer ever more possibilities. Unfortunately, the number of potential data security holes also grows, thanks to new applications compromising the integrity of users' resources by mindless design or irresponsible implementation.

It looks like the idea of widely available, safe computing is no closer to realization than it was, say, ten years ago. New 'scandalous' facts are revealed and discussed, with results which range from quick and effective fixes, through 'temporary' patches, marketing exercises attempting to paint a serious bug as a curious 'feature', to shifting responsibility for finding a cure to other developers.

" Blackmail for a good cause, some might say "

For someone involved in the computer security field, discovering a new, potentially dangerous and wide open security loophole can be extremely exciting. At the same time, the person who makes the discovery may find themselves with a personal moral dilemma which tests their professional integrity or even exposes them to possible litigation.

Let's check what possible actions they can take having made such a serious discovery. Although every case has a different potential impact on users and different solutions, it seems there are some possible reactions applicable to most scenarios:

- don't say anything to anyone
- contact the developer involved and explain the problem
- discuss the discovery in a limited environment (e.g. specialist mailing list)
- present and explain the issue to as many users as possible by all possible means

The first, and I think extreme, reaction must be based on the naïve hope that no one else will discover the problem, or abuse it. The former seems unlikely, given the number of organized and individual researchers, and implementing an evil idea is too tempting for plenty of the 'bad guys' out there. It is similarly naïve to assume that keeping the matter quiet means no one will ever be exposed to the danger. If there is a possibility, sooner or later someone will be hit, by chance if not intentionally. Thus, it is obvious that inaction does not solve anything.

The second approach seems ideal but only with the guarantee the developer will listen, understand the threat and do their utmost to fix the problem by providing users with a more secure environment. In reality, powerful developers only listen if they themselves face potentially damaging consequences by ignoring all warnings. The only serious threat to big corporations is a profit loss, and bad publicity (especially if based on truth) is one way to get it. Thus, the twin fears of bad press and loss of user confidence may be the main reasons some developers fix such problems (if a security vulnerability means nothing to them). It seems the threat of spreading the bad news may be necessary to make the big developers listen and act. Blackmail for a good cause, some might say.

The image of developers reacting (or being blackmailed and then reacting) to the findings of thousands of individual, enthusiastic, amateur researchers seems unreal, somehow. A specific security glitch has a much better chance of being addressed and fixed if it is backed by qualified professionals who have a chance to discuss and verify the problem. They may have some good ideas on the ways the improvement should be implemented.

This must be the ideal scenario; a problem is discovered, discussed and verified by independent and qualified researchers. It is then presented to the developers and, finally, swiftly addressed and fixed. Although this model, admittedly unattainable in real life, sounds like the best one, there remains one important question: what about users? Do they have the right to know the full implication of the danger they are exposed to? Is it fair to conceal the full mechanism and the meaning of the security hole in order to protect them from those among them who would abuse the faulty implementation and put their data at risk? What you don't see, can't hurt. Or can it?

Jakub Kaminski

NEWS

Method or Madness?

On 9 April *Network Associates Inc (NAI)* announced the start of lay-offs that will eventually account for approximately ten percent of its 1800-strong workforce. Most job losses are said to be in the administrative, corporate and marketing arenas, involving the closure of several 'redundant' [*surely not a pun? Ed.*] offices. These lay-offs coincide with moves to relocate some staff to corporate headquarters in Santa Clara, California.

A company spokesperson described the restructuring as a move to a 'tighter level of integration'. This is interesting in light of further claims that *NAI* is looking to hire a further 1000 people, mainly in consulting, sales and support roles.

Virus Bulletin also notes that during the last couple of months, a US recruiting firm has been advertising several positions for anti-virus software developers and researchers in Portland, Oregon. Further, a Portland-based head-hunter (judging by the 503 area code in his phone number) has been feeling out the potential skill pool for the position of head of anti-virus research at *NAI*. Together these observations suggest that the *McAfee* anti-virus team is moving to Portland. We wonder how this fits the model of 'tighter integration' in the official *NAI* spin control? ▮

Reflex Action

Dr David Aubrey-Jones, occasional contributor to *Virus Bulletin* and a familiar face at our annual conferences, has left the organization of which he became Technical Director in 1991. He resigned from *Reflex Magnetics Ltd* immediately before Easter. When asked the immortal question 'Did you jump or were you pushed?', Dr Aubrey-Jones provided *Virus Bulletin* with the following exclusive comment.

'I've enjoyed being part of *Reflex*. It has been exciting creating *Disknet* and building the security side of the business from nothing. However, after six and a half years I feel it's time to move on. I want to explore new challenges and opportunities, and so that's what I am doing.' ▮

Pastures New

Still on the subject of staff changes, *Virus Bulletin* has said a reluctant 'bon voyage' to Alie Hothersall, our subscriptions manager. She will be sorely missed by her colleagues and by all who attended her cheerfully and professionally managed VB'97 conference in San Francisco.

Virus Bulletin extends a hearty welcome to her replacement, Jo Peck and to our new software tester, Matthew Ham, who managed the comparative and *AVP* reviews this month. Both have tough acts to follow, but have already proved themselves to be worthy additions to the *VB* team ▮

Prevalence Table – March 1998

Virus	Type	Incidents	Reports
CAP	Macro	70	17.4%
Laroux	Macro	28	6.9%
Form	Boot	24	6.0%
AntiExe	Boot	23	5.7%
Concept	Macro	19	4.7%
Wazzu	Macro	15	3.7%
Monkey	Boot	14	3.5%
Npad	Macro	14	3.5%
NYB	Boot	13	3.2%
Parity_Boot	Boot	13	3.2%
Ripper	Boot	13	3.2%
DelCMOS	Boot	10	2.5%
Showoff	Macro	8	2.0%
AntiCMOS	Boot	7	1.7%
Dodgy	Boot	7	1.7%
MDMA	Macro	6	1.5%
Sampo	Boot	6	1.5%
Temple	Macro	6	1.5%
WelcomB	Boot	6	1.5%
Eco	Boot	4	1.0%
Johnny	Macro	4	1.0%
Junkie	Multipartite	4	1.0%
Stoned	Boot	4	1.0%
Appder	Macro	3	0.7%
Burglar.1004	File	3	0.7%
Edwin	Boot	3	0.7%
Galicia	Multipartite	3	0.7%
Stealth_Boot	Boot	3	0.7%
TPE	File	3	0.7%
Others [1]		67	16.6%
Total		403	100%

[1] The Prevalence Table includes two reports of each of: ABC, Baboon, Bleah, Da'Boys, DZT, Exebug, Impost, INT10, Jerusalem, Kampana, Kompu, Michelangelo, Natas, Niceday, Offspring.1135, Spanska.1000, Spirit and Yesmile.4304; and one report of each of: ABCD, Beer.3399, Byway, Cascade.1701, Counter, Gas, Helper, Jumper.B, Keypress-1216, Komcon, Minimal, Muck, Munch, Nightshade, Nottice, Pieck, Rapi, Razer, Schumann, Since, Switcher, Tentacle.1966, TPVO.3783, Trackswap, Umbrage, Unashamed_II, USTC.7680, Virogen.Pinworm, V-Sign, Wolleh.b and Yaka.

VIRUS BULLETIN **©1998 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England. Tel +44 1235 555139. /98/$0.00+2.50**

IBM PC VIRUSES (UPDATE)

The following is a list of updates and amendments to the *Virus Bulletin Table of Known IBM PC Viruses* as of 9 April 1998. Each entry consists of the virus name, its aliases (if any) and the virus type. This is followed by a short description (if available) and a 24-byte hexadecimal search pattern to detect the presence of the virus with a disk utility or a dedicated scanner which contains a user-updatable pattern library.

Type Codes

- **C** Infects COM files
- **D** Infects DOS Boot Sector (logical sector 0 on disk)
- **E** Infects EXE files
- **L** Link virus
- **M** Infects Master Boot Sector (Track 0, Head 0, Sector 1)
- **N** Not memory-resident
- **P** Companion virus
- **R** Memory-resident after infection

Ai22.1659

CER: A 1659-byte virus containing the encrypted texts 'C:\COMMMAND.COM', '.COM' and '.EXE'. Infected files have the text 'Ai22' at the end of code and their time-stamps set to 62 seconds.

```
Ai22.1659           B97B 062E 8B9C 5E07 B440 CD21 E8AF FB2E 8F84 7607 2E8F 846D
```

Animo.518

CN: An appending, 518-byte, fast, direct infector with the texts '*.ZOM', '[Animo]' and '[Rajaat/29A]'.

```
Animo.518           3681 76FA 9A02 3681 7EFA C04F 7503 E911 0036 817E FAD7 5875
```

Aref.670

CR: An appending, 670-byte virus containing the encrypted text '"Aref V.2.0" sends the greetings and deep regards to U. he is looking for someone to talk to, please contact to the following EMAIL address : Aref@REMOVED.CMOS.DATA ! Sig: Aref.K.1998 ;)'. The payload, triggering on the sixth day of every month, destroys the CMOS data and displays the above message. The virus disables the mouse support and printing (returning the 'out of paper' error).

```
Aref.670            3D99 9975 0293 CF3D 004B 7558 601E B001 33C9 B443 CD21 B43D
```

Aref.890

CER: An appending, 890-byte virus containing the texts '<< Towards a better tomorrow! >>' and '[AREF V.3.0]'. The payload, triggering on the fourth day of every month, destroys the CMOS data and displays the second message.

```
Aref.890            3D99 9975 0293 CF9C 3D00 4B75 6160 1E06 B001 33C9 B443 CD21
```

Aznar.666

CR: A prepending, 666-byte virus containing the texts 'COMEON' and 'VIRUS ANTI-AZNAR por JoDT VM'. Infected files have the string 'JoDT' at offset 0003h.

```
Aznar.666           B99A 02BA 0001 0E1F B440 2E8B 1E70 03CD 21B8 0242 33C9 33D2
```

Cachaca.400

CN: An encrypted, appending, 400-byte, fast, direct infector containing the texts 'El Virus ANTI-CACHACA ha entrado en acción.', '*.COM' and 'AntiCachaca Virus, escrito por el metalero Xavirus Hacker No escuche cachaca. Oiga Heavy Metal y vivirá mil años!!!'.

```
Cachaca.400         E880 01B9 B500 8DB7 5701 568B FEAD 3387 5501 ABE2 F8C3 ????
```

China.882

CR: A prepending, 882-byte virus containing the texts 'CHina CHina' and 'My Mother ,I Love you !'. Infected files have the string 'CHINA' at offset 0003h.

```
China.882           3D00 7F75 04B0 FF9D CF3D 004B 7406 9D2E FF2E 0D00 5053 5152
```

Die

CR: Two variants of an appending virus containing the encrypted text 'FOR BEAUTIFUL GIRLS! If you listen Alice Cooper Then I stuned with you now. Come my pussy pussy girl, I want kiss your lipsy now. (c) Light General.' Infected files have the word 2424h ('$$') at offset 0003h.

```
Die.490             B440 B9EA 0133 D2CD 2172 1026 C745 1500 00B4 40B9 0500 BA3F
Die.513             B440 B901 0233 D2CD 2172 1026 C745 1500 00B4 40B9 0500 BA56
```

Exeheader.360B

ER: A 360-byte virus placing its code in the unused space in headers of EXE files.

```
Exeheader.360B      B813 35CD 21BA 4001 B425 CD21 8BD3 BBAE 018C 4F04 061F B0CD
```

JDay.412

CR: An appending, 412-byte virus residing in the Interrupt Vector Table. It contains the encrypted texts 'Mike greets the world...', '<The Judgement Day>' and 'Now another file is infected...'. Infected files have the byte 4Dh ('M') at offset 0003h.

```
JDay.412            B440 B99C 0190 BAE0 01E8 7EFF B800 4233 C999 E875 FFB4 40B9
```

Kure.5337

CR: An appending, 5337-byte virus containing the text '[KURELUQUE Virus] Coded by Xavirus Hacker. Picture by Insane ¡¡¡Arriba Sportivo Luqueño Campeón!!! Un día como hoy, nació el glorioso club { MADE IN LUQUE - PARAGUAY }'. It infects files on opening (e.g. on COPY or TYPE commands). Infected files have their time-stamps set to 62 seconds.

```
Kure.5337           2D03 00A3 4501 B440 B9D9 1433 D2CD 21B8 0042 33C9 99CD 21B4
```

Lancelot.342

CR: A 342-byte prepender containing the text '[Sir LANCELOT du Lake Virus] (c) Programmed by Sir INT13H du Madness Kingdom of Paraguay'. Infected files have their time-stamps set to 60 seconds.

```
Lancelot.342        9A02 7630 A341 01B4 40BA 5602 B956 01CD 21B8 0042 2BC9 99CD
```

Light.1060

CEN: An appending, 1060-byte direct infector containing the text '(c) Light General.Kiev.1995.For free use!'. Infected COM files have the word 2424h ('$$') at offset 0003h and infected EXE files have the word 7878h ('xx') at offset 0012h.

```
Light.1060          BA00 01B9 2404 B440 CD21 33D2 2689 5515 2689 5517 C3B8 2012
```

Paraguay.1650

CER: A polymorphic, stealth, appending, 1650-byte virus containing the texts '#VIRUS A.J.V.M.#', 'Hi, I am AJVM. Nice to kill you, friend.', 'PaRaGuAy RuLeZ!', 'ANTI-VIR.DAT', 'CHKLIST.MS' and 'CHKLIST.CPS' Infected files have their time-stamps set to 32 seconds. The following template may be used for detection in memory only.

```
Paraguay.1650       B440 B972 06BA 7406 9C0E E81F 0226 C745 1500 0026 C745 1700
```

Paraguay.1726

CER: A polymorphic, stealth, appending, 1726-byte virus containing the texts 'Read ORDER.DOC for registration', '[HEAVY_METAL Virus] by Int13h. Random Damage Code by DARK AVENGER!', 'ANTI-VIR.DAT', 'AVP.CRC', 'CHKLIST.MS' and 'CHKLIST.CPS'. Infected files have their time-stamps set to 60 seconds. The following template may be used for detection in memory only.

```
Paraguay.1726       B440 B9BE 06BA CB06 CD21 26C7 4515 0000 26C7 4517 0000 B440
```

Paraguay.2283

CER: A polymorphic, stealth, appending, 2283-byte virus containing the texts '[ANTICPAV] by Int13h. MADE IN PARAGUAY', 'ANTI-VIR.DAT', 'CHKLIST.MS', 'CHKLIST.CPS' and 'AVP.CRC'. Infected files have their time-stamps set to 62 seconds. The following template may be used for detection in memory only.

```
Paraguay.2283       B440 B9EB 08BA EB08 CD21 E844 00B4 40B9 0300 BADA 02CD 212E
```

Paraguay.2618

CER: A polymorphic, stealth, appending, 2618-byte virus containing the texts 'C:\WINDOWS', '???????????', 'ANTI-VIR.DAT', 'CHKLIST.MS', 'CHKLIST.CPS', 'This program was written in the City of Luque - Paraguay - South America.', 'Dedicated to the memory of Kurt Cobain.', 'COBAIN! Virus, programmed by Int13h.', 'Hey, with this card you can't see some graphical effects of viruses :-(', 'Buy a VGA card! Next time you'll be punished under Viral Law #1632.', 'You was warned by COBAIN! Virus, coded by Int13h in Paraguay.' Infected files have their time-stamps set to 32 seconds. The following template may be used for detection in memory only.

```
Paraguay.2618       B440 B93A 0ABA 470A CD21 26C7 4515 0000 26C7 4517 0000 B440
```

Paraguay.2867

CER: A polymorphic, stealth, appending, 2867-byte virus containing the texts 'VIRUS PARAGUAY Ver. 3.0!', 'Programmed by Int13h, in Paraguay, South America.', 'ANTI-VIR.DAT', 'CHKLIST.MS', 'CHKLIST.CPS', 'AVP.CRC', 'C:\COMMAND.COM', 'C:\WINDOWS' and '???????????'. Infected files have their time-stamps set to 60 seconds. This template may be used for detection in memory only.

```
Paraguay.2867       B440 B933 0BBA 3E0B CD21 26C7 4515 0000 26C7 4517 0000 B440
```

Scrm.1216

CER: A stealth, encrypted, appending, 1216-byte virus containing the text 'Bill Yang?!Fuck up, Bill is SCRM of a community! This is Evil God of Virus/Taipei/Taiwan'.

```
Scrm.1216           B98B 04B0 ??D0 C8F6 D82E 3004 02C0 46E2 F4C3
```

Spooky.323

CR: A 323-byte appender, which resides in the Interrupt Vector Table. Infected files have the word 5350h ('PS') at offset 0003h. On 25 December it overwrites 20 sectors on the first hard disk.

```
Spooky.323          B440 B943 018B D681 EA85 00CD 2158 2D03 0083 EE14 8904 83C6
```

Strato.1597

CR: A stealth, encrypted, 1597-byte appender containing the texts 'Dedicated to the great finland group of purified heavy metal Guitars (speed-of-the-light): Timmo Tolkki Vocals: Timmo Kotipelto Bass: Jari Kainulinez Drums: Jörg Michael Keyboards: Jens Johansson Fright Night - Twilight Time - Dream Space - Fourth Dimension - Episode - Visions', '[STRATOVARIUS Virus] (c) Copyright Int13h 02/08/97', 'MaDeInPaRaGuAySoUtHaMeRiCa', 'anti-vir.dat', 'chklist.ms', 'chklist.cps' and 'avp.crc'.

```
Strato.1597         CC8B 6EFA 81ED 0301 F7D4 F7D4 8DB6 2001 568B FEB9 0E03 AD35
```

Suela.1042

CER: An encrypted, appending, 1042-byte virus containing the texts 'C:\COMMAND.COM' and 'Runing [Suela]-DOS System v1.0. Please wait...'.

```
Suela.1042          ??BE ???? B9F4 032E 8A44 012E 3004 46E2 F6C3
```

Tout.275

CN: An encrypted, appending, 275-byte, fast, direct infector containing the text '*.cOm' and 'A toute le monde!'. Infected files have their time-stamps set to 62 seconds

```
Tout.275            8DB6 3801 56FC 8B96 1A02 B971 008B FEAD D2CE 33C2 ABE2 F8C3
```

TripleK.471

CR: An appending, 471-byte virus containing the text 'Triple_K Virus by Int13h. Coded in Paraguay. Kai + Kiske + Keeper = KEWL! HELLOWEEN db 'The best Heavy Metal group of the universe''. Infected files have the byte 4Bh ('K') at offset 0003h.

```
TripleK.471         B440 33D2 B9D7 01CD 21E8 1900 B440 B904 00BA 3701 CD21 B43E
```

XRes.432

ER: An appending, 432-byte virus. Infected files start with the word 4D5Ah ('ZM').

```
XRes.432            60B4 40B9 B001 33D2 CD21 B800 4233 D233 C9CD 21E8 2300 80EC
```

Vanitas.3712

ER: A polymorphic, 3712-byte appender containing the texts 'C:\COMMAND.COM', 'Have a nice death...', 'C:\WINDOWS\COMMAND.COM', 'VANITAS++ v2.0 GR(c)97 by ANAX. [E-75] goes to Hell.'. Infected files have the word FACEh at offset 0012h. This template is for detection in memory only.

```
Vanitas.3712        B800 37BB CEFA CD21 3DCE FA75 03E9 1601 E834 04B8 8716 CD2F
```

VIRUS ANALYSIS

Caught Red-handed

Sarah Gordon with Frédéric Perriot
IBM

At the 1997 Virus Bulletin Conference in San Francisco, I gave a joint presentation with Joe Wells on 'Hypes and Hoaxes'. The paper detailed ways in which you can curtail the spread of hype and hoax within your organization, such as encouraging scepticism and designating a central authority for information on viruses. Other methods include learning to spot the signs of a hoax, such as misspelled words and 'technobabble', and not obeying the request to 'pass this message along to as many people as possible'.

So, if a message contains misspelled words, technobabble and encourages you to pass it on to all your friends, surely the whole thing is a complete hoax, right? Wrong. Well, sort of. Please read on.

Enter RedTeam

Shortly after the publication of the VB'97 paper, I received (presumably from the virus writer or one of his associates) a package that contained what appeared to be the first ever virus that used *Eudora* to spread itself via email – Win/RedTeam. As *Eudora* is a very popular email application package, and the virus appeared less buggy than ShareFun (see *VB*, April 1997, p.10), I was at the same time both alarmed and curious.

However, as this new virus was not actually found in the wild when I first saw it and it was only in source code form, I did not see any reason to make much fuss about it. I put it on the back burner – that is, until enquiries regarding this virus started flowing in.

What prompted the flurry of concern? One company issued a 'virus alert' press release about it. The virus had been seen on a virus exchange site, and I have since heard (as yet, unsubstantiated) claims that it has spread throughout organizations. It is this last detail that particularly interests me, because the 'spread factor' of this virus could be decreased by awareness of the 'hoax factor' I talked about in San Francisco.

Presentation is Everything

Win/RedTeam functions as a fairly normal parasitic file-infecting virus, with one important addition. If *Eudora* is installed on the host machine, the virus attempts to send an email to other users. This email consists of several paragraphs of text, followed by a binary attachment called 'K-RTEAM.EXE'. Before examining the program, let us look at the email message. The subject of the message is 'Red Team' – more about that in a moment. The email message that the virus sends out is reproduced in the text box below. The emphasis here is mine. The actual text (including spelling mistakes) is exactly as it would appear to a person receiving a message from this particular variant of the RedTeam virus.

```
Subject: Red Team
Cc:
Bcc:
X-Attachments: C:\K-RTEAM.EXE

Hiya!

Just thought I'd warn you about a destructive new e-mail virus.
Here is some info:

> The "Red Team" virus is a complex new computer virus that spreads via
> the Microsoft Windows operating system, and Internet E-Mail. Although
> it is not the first virus to spread via E-Mail (that was "Good Times"),
> the Red Team virus is unparalelled in its destructive capabilities.
> Further more, the virus is exceedingly common - it has already been
> reported in much of western Europe, the USA, Russia, Australia, and
> Japan. In short, everywhere.
>
> We at QUEST, have spent several weeks analysing this virus, and are proud
> to anounce that we finally have a cure! The program, named "K-RTEAM"
> (Kill Red Team), can be executed in any Microsoft Windows environment, and
> will reliably detect (and remove if nescessary) the Red Team virus from
> your system buffers.
>
> -
> Julia Blumin
> QUALCOMM Enterprise Software Technologies
> World Wide Web: http://www.qualcomm.com

The reason I thought I should warn you, is that we recently had a run in
with this beast.  Luckily we managed to get a copy of the excellent
'K-RTEAM' programme before the destruction really started. Just in case
you should suffer the same misfortune, I have included this programme for
you too.

Bye!

P.S. Make sure you warn all your friends of this new threat!
```

The message seems to contain rather subtle and sometimes not-so-subtle indications that this whole thing just might be a setup. First, we note the somewhat subtle reference to *Qualcomm*. *Qualcomm Inc* is a supplier of digital communications products. One of these is *Eudora* – the very program RedTeam uses to facilitate its spread.

It is this seamless functionality which provides RedTeam with an additional boost in virulence, and it is a touch of irony that the message claims to have originated with *Qualcomm*. There is more! Did you notice something else strangely familiar about the email message?

Mass destruction, misspelled words and technobabble – this is sounding more and more like a hoax with every word. There is the reference to Good Times as the first email virus. We *all* know by now that was a hoax. Using the virus name in the cure is in rather poor taste – why give the bad guys any satisfaction at all? Surely none of us would make that error, and risk paying homage to the enemy. The spelling errors and the technobabble about removing the virus from system buffers give a strong indication that this message is not the work of an IT professional. The final blow, however, must be the plea to 'warn all your friends'.

So, could this whole thing be a fake? Unfortunately, this is not quite the case. Attached to the message is a 6351-byte file called K-RTEAM.EXE, which the message claims is a 'cure'. There really *is* a RedTeam virus, but the way it attempts to spread from machine to machine is by tricking you into believing the email message you have just received, and deciding that you should execute this 'cure'. If you do detach and run this program, the virus will infect the system, and try to send out email about itself to some of the people in your address book. Now, the question is, of course, 'Will users actually react this way?'

This is where things become a little more complicated. As mentioned earlier, one anti-virus company distributed a 'virus alert' concerning RedTeam recently. The alert stated factually that the new virus infects computers and emails itself, using *Eudora*, and went on to say 'We feel that this virus has the potential to spread quickly and infect users around the world'. It was followed by numerous posts to alt.comp.virus discussing the 'first email virus' and heightening public awareness of RedTeam.

With all this attention, it is reasonable to think that people may well want to find cures for this virus. Will the method they choose to use be the 'disinfector' that arrives with a message about the virus? Users know not to take candy from strangers, and that opening documents or executing programs from strangers can lead to problems – but the messages RedTeam sends will come from people who are known to them. People who have them in their personal *Eudora* address book.

I do not know a great deal about *Eudora*, and in fact have never used it. So, while I knew the RedTeam virus I had received replicated and in fact did contain what appeared to me to be everything it needed to do the apparent bidding of its author, whether or not it actually worked with *Eudora* was a mystery. Fortunately, Fred Perriot, from our immune system lab was happy to explore this. I gave him the samples and he retreated to his lab. He emerged with the following analysis of the virus, which includes a description of its interaction with *Eudora*.

Inside RedTeam

RedTeam is a parasitic file infector. It targets *Windows* files with the NewEXE format (*Windows* 16-bit segmented executables). The virus has two infection methods – one used for normal files, where the virus hooks the entry point, the other used for kernel files (KRNL386.EXE), where the virus hooks the WINEXEC or the INITTASK function. When run from a normal file, the virus just infects the *Windows* kernel then executes its host. It may also create the file 'K-RTEAM.EXE' and its accompanying email message and queue them for sending to other machines. When run from the kernel, the virus goes resident and infects files as they are executed. Infected files have a length that is a multiple of 73 bytes and the virus refuses to infect potential hosts matching this criterion.

RedTeam's infection method is complex but effective. Instead of simply appending itself to its host, the virus inserts itself in the entry segment of the host, just before the relocation table. Everything after the code segment in the host is shifted toward the end of the file by the size of this 'hole'. Such an infection method involves considerable manipulation of the headers and the various other tables to keep the offsets of the many sections in line with the new file contents. The virus does this successfully, as infected programs run well under *Windows 3.x* and *Windows 95*.

During the kernel infection, the virus differentiates between the *Windows 3.x* and *Windows 95/NT* kernels by looking for the CallProc32W function in the non-resident name table of the kernel. In the *Windows 3.x* kernel, the virus targets the WINEXEC function, adding itself to the WINEXEC entry segment. In *Windows 95/NT*, the virus was designed to target INITTASK but in fact the infection fails because of a trivial error. As a result it fails to find the INITTASK entry and aborts the kernel infection.

The author seems to have been very cautious. The virus contains checks to avoid infecting DLLs, font files, ill-behaved *Windows* applications, etc. After performing a file infection, the virus fixes the module table in memory to reflect the new structure of the file image on the disk. Interestingly enough, under *Windows 3.x* the virus infects applications in the background, which makes its presence in memory hardly noticeable, even on slow 386 machines.

The virus body contains the compressed mail message and uninfected dropper. The *Eudora* routine starts by opening some *Eudora* files. If these file opens succeed the virus creates an empty file, RTBASE.TOC, that serves as a marker to avoid sending the email message to the same

person twice. It then decompresses the dropper and infects it. This results in a 6351-byte long file 'C:\K-TEAM.EXE', to be used as an attachment. The message text is then decompressed and a new *Eudora* message, addressed to all the names in the NickName database (NNDBASE.TOC), is created. It finally appends the mail to the OUT.MBX file and creates a reference to it in the OUT.TOC file, indicating that the mail ought to be sent.

Coming to a PC Near You Soon?

RedTeam leaves us in a quandary in terms of assessing the threat it poses to our machines. In one sense, its proactive ability to hop from machine to machine via email gives it a handy extra vector for infection. However, the virus can only make use of *Eudora* and explicitly requires you to launch the infected attachment. How well it could spread depends initially on whether or not you recognize that the message bringing the cure is a hoax. Again, the best initial defence against this type of threat is to make sure you encourage scepticism, designate a central authority for information on viruses and learn to spot the signs of a hoax, such as misspelled words and technobabble.

Unfortunately, the warning to 'pass this along to your friends' is something that RedTeam does for the receiver (if they use *Eudora* and run the attachment). However, with the right policies in place, you can avoid this happening, as your users will not execute the 'cure'.

Is this the end of computing as we know it? We think not. It is, however, a disturbing indication of what may be to come. So, next time someone you know sends you an attachment unexpectedly, look at it with a certain amount of suspicion. Do you really know what that program will do?

RedTeam

Alias:	Win/RedTeam.4766.
Type:	Resident new-EXE file and Windows kernel infector.
Length:	4766 bytes.
Self-recognition in Files:	File length is a multiple of 73 bytes.
Hex Pattern in Files:	`41C5 75AF C928 DB49 B159 EADC 5C77 34B9 C666 6E94 381D 74AE BD87 2451`
Trigger:	When run from kernel, Eudora is installed and RTBASE.TOC marker file is not present.
Payload:	Attempts to mail itself to all addresses found in Eudora address book.
Disinfection:	Under clean system conditions, identify and replace infected files.

TUTORIAL

Free Macro Anti-virus Techniques – Part 2

Jimmy Kuo
Network Associates Inc

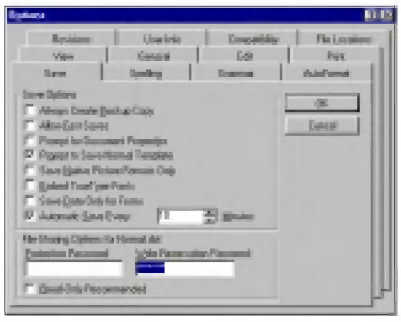
[*In this installment of his self-help series, Jimmy continues with more options for protecting your NORMAL.DOT file. Remember that unless otherwise stated, file locations are the* Word 95 *defaults and may vary for* Word 6 *and/or* Word 97 *users. Ed.*]

Password Protect NORMAL.DOT

Adjacent to the Read-Only Recommended option on the Save tab of Tools, Options (see *VB*, April 1998, p.12) is Write-Reservation Password (or Password to modify in *Word 97*). If this choice is invoked, the user will be asked to enter the password or open the file as read-only, each time *Word* is started.

The advantage of this is that only certain people will be allowed to modify NORMAL.DOT, if and when they wish to. The disadvantage is that only the same few people can clean up an infection. If NORMAL.DOT is allowed to be infected, no warning is given.

To set this option, start a *Word* session and explicitly open the NORMAL.DOT file (usually located in the folder \MSOFFICE\TEMPLATES). Click on Options on the Tools menu and choose the Save tab. At the bottom, on the left, in a box entitled File-Sharing Options for normal.dot, type a password into the Write-Reservation Password box. You will then be asked to confirm the password. Type in that same password again. Close the editing session, exit and save all changes.



Pro: Allows flexibility for a select few who want their NORMAL.DOT to be read-only at certain times.

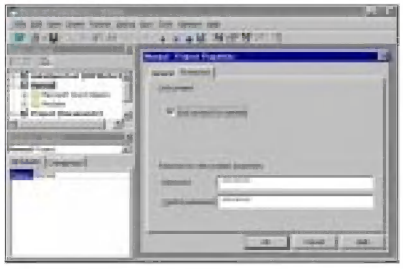
Con: Sends a message to you each time you start *Word*.
Only a select few can clean up the global infection.

Lock VB Project for NORMAL.DOT (Word 97)

There is yet another method to make NORMAL.DOT a write-protected document for *Word 97* users. This feature prevents modules from being created, viewed, or copied

into the Template Project. Macro viruses, which are Visual Basic modules, fall into this category. However, font selections, AutoText, and other stylistic choices and settings do not. Thus, a user could change certain default choices in NORMAL.DOT without having to overcome protections, and still not allow a standard macro virus to infect.

To set this up, make sure NORMAL.DOT is writable, then start a *Word 97* session. Press Alt-F11 to open the Visual Basic Editor, then click Project Explorer on the View menu. Click on Normal to select it. Next, click on Tools, Normal Properties and choose the Protection tab. Check Lock project for viewing, set a password then click the OK button. From the File menu click Save Normal, then Close and return to Microsoft Word. Finally, exit from *Word*.



Pro: Virus cannot bypass this unless it happens to guess your password.

Users needing to change Autotext and Toolbars will not be affected.

Using the Operating System to Advantage

Probably the most effective thing you can do for yourself is change the attribute of NORMAL.DOT to read-only. As it is so easy to do and quite effective, it is also the most talked about method on the Internet. Hopefully, many of you already have this in place in one form or another.

DOS has the concept of attribute bits. The most commonly referenced are the System, ReadOnly (RO), Hidden, and Archive bits. The specific attribute bit which interests us is the ReadOnly bit. If the RO bit is set, normal DOS system calls will refuse to write or change the file. Thus, in theory, if the NORMAL.DOT file is ReadOnly, no virus will be able to change it.

As noted before, a virus usually wants to change the global environment. This generally causes the NORMAL.DOT to be rewritten. However, if the RO bit is set, *Word* recognizes and stores this fact when it opens NORMAL.DOT. When *Word* exits, it remembers NORMAL.DOT was ReadOnly and makes no attempt to change it.

If it is such a good idea to set the read-only bit, why doesn't everyone do it? What is the downside? The most obvious consideration is, 'the file is read-only.' It cannot be changed, not even intentionally.

A ReadOnly NORMAL.DOT severely cramps the productivity of someone who often changes their NORMAL.DOT. It would seem that such a user cannot benefit from this technique, but that is not entirely true. Macro users can still operate with a ReadOnly NORMAL.DOT, by storing all their macros in files in the Startup directory. This would involve a change in their normal mode of operation. Macros would be handled in the same way as NOAUTO.DOT (see *VB*, April 1998, p.11).

A second and very important note is that you will not realize a virus is active until after exiting *Word*. A significant technical point is to recognize that *Word* informs you of the attempt to write to NORMAL.DOT when it exits (assuming you have enabled the Prompt to Save Normal Template option – see *VB*, April 1998, p.10). So, all the time you are using *Word*, files will merrily continue to be infected without warning.

You know for sure on exit, and you can shift into 'virus forensics' mode immediately, should such a warning arise. Forensics need as much historical information as can be mustered. To facilitate this, you need to make use of the Most Recently Used (MRU) list. By default, *Word's* MRU list is set to remember the last four files that were opened. These are going to be the files of interest anyway; the files saved on that day are the ones to be tracked down if they have been sent to someone.

With a default of only four, the length of the MRU list needs to be increased. To do this in *Word*, choose Tools, then Options, then General. Go to the Recently Used File List and increase the number to its maximum of nine (remembering to check the item).

Pro: Good system level protection.

Slows down viral spread.

You will know of infection within the day, and it enables activity tracking.

A virus cannot circumvent this to infect NORMAL.DOT in the same session.

More files are available in the MRU list.

Con: If you have to update macros constantly, productivity will be hindered.

This can create a false sense of security.

Acknowledgments:

Vesselin Bontchev, *FRISK Software International*; Ray Glath, *RG Software Systems*; and Stefan Geisenheiner, Jivko Koltchev, Akihiko Muranaka and François Paget, *Network Associates*.

A version of the original paper from which this series is derived is available from *Network Associates'* web site at http://www.nai.com/services/support/vr/free.asp. That paper is available in English, German and French.

COMPARATIVE REVIEW

Windows of Opportunity

Another *Windows 95* comparative. We hear you asking: Can it have been six months already? Well, technically it is, but it is less than that since *Virus Bulletin* published the last *Windows 95* comparative. A major contributory factor to the delay in publication of that review was that more than a few fairly major annoyances made themselves felt during testing. Then, while compiling the final results for publication, it seemed that re-testing some products under the same conditions would lead to different results. This was most perplexing, and after failing to resolve why some products behaved like this, we eventually published results that were typical of those seen in the actual tests.

That was not an ideal situation. This time we are playing truth or dare. The vendors who dared submit poorly tested or otherwise inadequate products may not like the truth revealed through the pages of this review. *C'est la vie*.

A reviewer's job is to review. A developer's job is to develop. It seems that some developers believe they can do their job without testing their products, or at least, they believe they need not test their products as thoroughly if they are making a special build to send out for review or testing. That seems a little like Russian Roulette to us, but from a developer's perspective it can make sense.

Anti-virus developers are always under pressure. There are always new viruses to add detection of to one's product. There are sometimes new forms of virus (as in recent months we have seen *mIRC* script, *Excel* formula and *Access* macro viruses arise – all covered in *VB*, April 1998, as chance would have it). The latter can add a significant burden to product developers, who now face possibly having to reverse-engineer a new file format, understand how another part of an OS works, and so on. However, developers are also under pressure to meet promises made to their marketing and sales departments – all those additional and better features, the nicer shade of blue in the splash screen and so on.

Possibly the worst pressure is that 'large new sale' that 'looks promising, so long as we have another good review'. *Virus Bulletin* has had subtle, and at times not so subtle, pressure applied by various vendors to 'test the newer version' so their product looks better in a comparative review. Just days before going to print with this issue, a senior executive at one of the major anti-virus developers said, almost tangentially to our conversation, 'you *do* know the latest updates are on our web site?'.

Unfortunately for us as testers, it appears that many developers yield to these sorts of temptations. We see products with quick fixes and many, perhaps not fully-tested, new virus definitions thrown in right up to the product submission date for the review. At that point, the developer burns a gold CD-ROM and writes the new version number on it with a marker pen.

This is not a complaint about gold CDs *per se* – many perfectly fine products arrive here in such a form, and it is understandable that with the product submission date for comparatives usually just a few days before the end of a month, some vendors may still be waiting to receive their product back from their reproduction plants.

It *is* a gripe about shoddiness. As potential purchasers of these products, *Virus Bulletin's* readers are entitled to see the warts. What follows is the 'no holds barred' version of a *Windows 95* comparative review. Not describing what goes into producing the apparently simple and sane statistics we usually publish does no-one any good in the long run. In the course of performing the current review, it was decided that as the warts finally outweighed the clear complexions, it was time to tell it like it is.

Test Procedures

At the end of February, a total of twenty-two products were submitted for testing, however, one of these proved completely untestable. As the February WildList was released a little later than usual that month (late on the last day the developers had for shipping their products to *VB*), the In the Wild Boot and File test-sets used for testing were updated to the January WildList.

The products were tested following individual installation on standard *Windows 95* workstations. These have their hard drives restored from sector-level backups between products. To ensure the integrity of the virus test-sets, they were stored on a *NetWare 3.11* server and the tests were run by a user who only had read and file-scan rights to the test-set directory.

For the on-demand detection tests, wherever possible, complete reports or detection logs were produced by the program under test, and then parsed for infection reports. In some cases this was either not possible or seemed to provide anomalous results. In these instances, the test-sets were copied to the test machines' hard drives and the software set to delete infected files. The samples remaining were deemed 'missed'.

On-access detection was also normally tested against the undisturbed samples on the server. To test this increasingly important mode of operation, the on-access component of the product under test is configured appropriately ('silent mode' is used if available, and the action on detection is set to deny access). Then a simple *Windows* program is employed. It runs through a directory tree trying to open all

On-demand tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Alwil AVAST32	87	100.0%	655	100.0%	100.0%	1134	98.7%	12998	95.4%	906	100.0%
Cheyenne Inoculan	86	98.9%	654	99.9%	99.5%	1021	89.1%	12679	91.7%	906	100.0%
Command AntiVirus	87	100.0%	621	97.6%	98.4%	988	86.2%	6968	47.0%	817	92.7%
Cybec VET	84	96.6%	655	100.0%	98.8%	1091	95.0%	13498	99.1%	900	99.3%
Data Fellows F-Secure Anti-Virus	87	100.0%	655	100.0%	100.0%	1142	99.3%	13499	99.1%	906	100.0%
Dr Solomon's AVTK	87	100.0%	655	100.0%	100.0%	1138	99.0%	13500	100.0%	906	100.0%
EliaShim ViruSafe	86	98.9%	653	99.9%	99.5%	995	86.9%	13163	95.4%	906	100.0%
ESET NOD32	87	100.0%	655	100.0%	100.0%	1127	98.1%	13500	100.0%	906	100.0%
GeCAD RAV	85	97.7%	620	97.5%	97.6%	1134	98.7%	13495	99.0%	868	96.7%
IBM AntiVirus	87	100.0%	655	100.0%	100.0%	1122	97.6%	13500	100.0%	906	100.0%
iRiS AntiVirus	86	98.9%	654	99.9%	99.5%	1056	92.1%	13083	94.0%	906	100.0%
Kaspersky Lab AVP	87	100.0%	655	100.0%	100.0%	1146	99.7%	13500	100.0%	906	100.0%
McAfee VirusScan	87	100.0%	655	100.0%	100.0%	1130	98.3%	13441	98.7%	888	98.8%
Norman ThunderByte	87	100.0%	655	100.0%	100.0%	1115	97.0%	13496	98.1%	883	98.1%
Norman Virus Control	87	100.0%	646	99.7%	99.8%	1120	97.4%	13495	99.0%	899	99.7%
Panda Antivirus	87	100.0%	628	96.2%	97.5%	833	72.4%	9344	68.6%	660	80.8%
Quarterdeck ViruSweep	86	98.9%	653	99.9%	99.5%	995	86.9%	13163	95.4%	906	100.0%
Sophos SWEEP	87	100.0%	644	99.4%	99.6%	1107	96.4%	13495	99.0%	904	99.7%
Stiller Integrity Master	85	97.7%	618	96.6%	97.0%	856	74.8%	5044	32.7%	743	85.6%
Symantec Norton AntiVirus	87	100.0%	655	100.0%	100.0%	1119	97.4%	12001	88.0%	891	99.1%
Trend Micro PC-cillin 95	83	95.4%	648	98.7%	97.6%	1053	97.4%	12964	94.2%	884	98.5%

files it finds (and closing them when successful). This utility logs file-open errors, and as no other programs are running concurrently and the test is run after a restart, errors are presumed the result of the scanner under test.

One test machine is reserved for timing and overhead tests. In this case, the Clean test-set is stored on the local hard drive and the workstation is disconnected from the network and restarted standalone. Elapsed scanning time is measured with a digital stopwatch. The overhead tests involve copying 200 executable files (part of the Clean test-set) from one directory to another on the workstation. A baseline measurement is made with all active components disabled (unloaded if possible) and then repeated with various configuration options enabled. Tests are repeated ten times under each condition, and an average recorded. The results for each product are normalized to 20 seconds for the baseline condition, before graphing.

The boot virus samples are all kept on write-protected, 3.5-inch diskettes. On-demand testing is performed from the test product's user interface. On-access detection tests are generally made by attempting to access the infected diskettes from the *Windows* Explorer (by clicking the appropriate drive icon). All manner of tricks have been found necessary to persuade the combination of *Windows*, Explorer and certain products to acknowledge that the diskette in the drive has changed. These include multiple

On-access tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Alwil AVAST32	87	100.0%	n/a		n/a	n/a		n/a		n/a	
Cheyenne Inoculan	84	96.6%	654	99.9%	98.7%	1021	89.1%	n/t		906	100.0%
Command AntiVirus	87	100.0%	621	97.6%	98.4%	988	86.2%	6969	47.1%	817	92.7%
Cybec VET	77	88.5%	655	100.0%	96.1%	1091	95.0%	13498	99.1%	900	99.3%
Data Fellows F-Secure Anti-Virus	87	100.0%	635	97.0%	98.0%	1075	93.6%	13499	99.1%	906	100.0%
Dr Solomon's AVTK	87	100.0%	655	100.0%	100.0%	1146	99.7%	12922	90.3%	906	100.0%
EliaShim ViruSafe	86	98.9%	653	99.9%	99.5%	995	86.9%	13163	95.4%	906	100.0%
ESET NOD32	85	97.7%	655	100.0%	99.2%	1127	98.1%	13500	100.0%	906	100.0%
IBM AntiVirus	63	72.4%	496	79.0%	76.8%	884	77.4%	0	0.0%	124	12.2%
iRiS AntiVirus	84	96.6%	654	99.9%	98.7%	1056	92.1%	n/t		906	100.0%
Kaspersky Lab AVP	87	100.0%	655	100.0%	100.0%	1146	99.7%	13500	100.0%	906	100.0%
McAfee VirusScan	51	58.6%	655	100.0%	85.9%	1067	92.9%	13275	93.2%	888	98.9%
Norman ThunderByte	84	96.6%	593	90.8%	92.8%	859	75.0%	n/t		897	99.3%
Norman Virus Control	82	94.3%	n/a		n/a	1143	99.4%	n/a		n/a	
Panda Antivirus	59	67.8%	560	87.5%	80.8%	837	72.7%	n/t		541	71.1%
Quarterdeck ViruSweep	83	95.4%	653	99.9%	98.4%	995	86.9%	13163	95.4%	906	100.0%
Sophos SWEEP	87	100.0%	653	99.4%	99.6%	1107	96.4%	13495	99.0%	904	99.7%
Symantec Norton AntiVirus	86	98.9%	655	100.0%	99.6%	1126	98.0%	13500	100.0%	906	100.0%
Trend Micro PC-cillin 95	83	95.4%	642	97.2%	96.6%	1034	90.2%	n/t		883	98.4%

disk swaps, accessing the drive from other applications and intermingling several non-infected diskettes among the sample diskettes.

So, how did everyone fare? Read on…

Alwil AVAST32 v7.70 (Build 702)

ItW Boot	100.0%	Macro	98.7%
ItW File	100.0%	Macro on-access	n/a
ItW File on-access	n/a	Polymorphic	95.4%
ItW Overall	100.0%	Standard	100.0%

AVAST32 provided a quiet beginning to this review, along with what came to seem like the unfamiliarity of a product which performed generally as advertised. Its dedication to the purpose at hand – detecting viruses – is justly rewarded with the first VB 100% award in this comparative review. *AVAST32* has an active component, but as we have noted in previous comparatives, *Virus Bulletin* is not geared-up to test products whose active components (reputedly) intercept infected programs at load-and-execute time. This 'limitation' has not changed, so only boot detection has been tested with on-access methods.

The usual collection of beetles graced *AVAST32's* virus alerts, and their only oddities were the boot sector results. The alerts are meant to inform you whether they are due to on-access or on-demand scanning, but if both are operating, confusion is often the result. On occasion, the on-access scanner produced alert boxes that did not have system focus, and were thus invisible behind the on-demand menu. This could only be produced reliably with MISiS, when the message 'a device attached to the system is not functioning' appeared upon scanning.

Another small problem was found, in that AVAST32's log files always seemed truncated or to just completely miss reporting a block of files that the on-screen status monitor had clearly shown being scanned (and found infected). It is suspected that this behaviour may be related to the log file size limitation option. Various settings, from just larger than necessary to many megabytes, did not substantially alter things here. Eventually, the full test-set was copied to the test machine and *AVAST32* asked to delete all infected files.

Cheyenne Inoculan v5.0 (Build 064)

ItW Boot	98.9%	Macro	89.1%
ItW File	99.9%	Macro on-access	89.1%
ItW File on-access	99.9%	Polymorphic	91.7%
ItW Overall	99.5%	Standard	100.0%

Inoculan managed, in the face of stiff competition, to be one of the most frustrating products yet received. Primary in this was its inability to produce any form of report file – binary log files were to be found in the program directory, but no option to produce plain-text or hard-copy reports was evident. Gobsmacked at such an omission, the reviewer assumed he was missing a subtlety in a menu somewhere. Unfortunately, recourse to the on-line help provided no relief – despite being clearly the English version, the review copy of the product was supplied with help files universally written in German! Nice and fully context-sensitive (as far as we could judge with our rudimentary grasp of that language), but nevertheless completely in German.

Perhaps we should have expected such quality from the outset, given that the first screen displayed by the installation program referred to the product as 'Incoulan'. A quality assurance program that does not prevent the misspelling of the product's name could almost be forgiven for providing only alternative-language help files.

Fortunately, an *Adobe Acrobat* PDF file of the English manual was discovered on the gold CD-ROM on which the product arrived. However, after some trolling around, it seemed that reporting the results of a scan was a capability beyond the scope of this version of the product.

On-demand boot sector testing was difficult, due to the product's insistence on performing memory checks prior to checking each diskette. Theoretically, this action could be disabled, but it was spontaneously reset by every virus detection that occurred. This is triggered by the product's default setting, which, upon detection of a virus, will set 'options for highest level of detection for 30 days'.

This seems like a good setting – in theory it increases a user's level of protection once evidence of greater risk is detected. It could be a nuisance in some situations though, unless it can be disabled. In fact, the option that claimed to enable and disable this escalation feature made no difference to performance – on detecting a boot virus, memory scanning was re-enabled. If the memory scan option was not manually deactivated after such a detection, there was a high likelihood the previous virus would be (technically erroneously) detected in memory before scanning the next sample diskette. When this happened, *Inoculan* insisted 'Virus in memory – Reboot with rescue disk'. It was thought that clicking the OK button then closing and restarting *Inoculan* would probably suffice at this point, but it transpired that the supposed warning message (just described) is, in fact, a request from *Inoculan* to restart the machine. As there was only an OK button, it was very onerous when one forgot to disable memory scanning between boot virus detections.

Attempts to test on-access detection across the *Virus Bulletin* collection resulted in a series of reboots and hangs. This could only be resolved, as in several other cases in this review, by splitting the collection into smaller chunks to be scanned separately, interspersing each test chunk with a system restart. Even so, the Polymorphic test-set remained untestable – it would appear that if you have more than a few hundred files infected with a polymorphic virus, you will have to run this product many times and with much finagling of options and locations to scan to obtain a clear picture of the extent of the 'damage'.

Inoculan also managed to have the worst problem with the Clean test-set. A simple false alarm was not lowly enough for *Inoculan*, however – it crashed completely upon scanning a particular file in the test-set. Replacing that file with one of very similar size saw *Inoculan* limp across the line with a time of 1931 seconds and a data throughput rate of 276 KB/second.

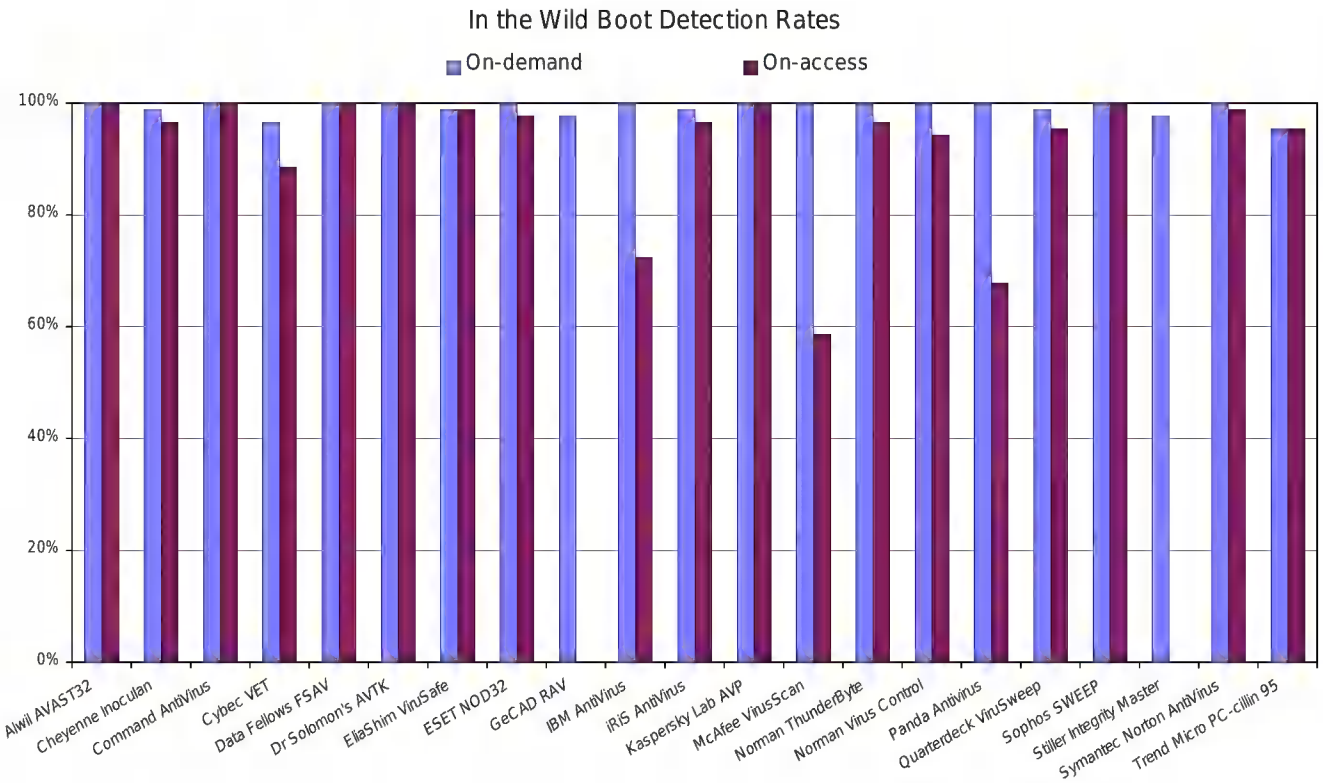
Given that *Microsoft* is known to license *Inoculan* as its corporate-wide anti-virus solution, *Virus Bulletin* hopes the reviewed product is not truly indicative of the anti-virus development efforts at *Computer Associates* since it took over *Cheyenne* (and thus the *Inoculan* product).

Command AntiVirus v4.0

ItW Boot	100.0%	Macro	86.2%
ItW File	97.6%	Macro on-access	86.2%
ItW File on-access	97.6%	Polymorphic	47.0%
ItW Overall	98.4%	Standard	92.7%

Command AntiVirus (*CAV*) proved a strange creation, but did not really qualify for the big league of irritations encountered elsewhere. Boot sector detection was good with 100% detection rates for both on-demand and on-access scanners. However, the program managed to detect a large number of the boot sector viruses *twice* on-access, despite only one method of scanning being active. Performance on all the other test-sets continues to slip with the newer *Word 97* macro viruses being especially challenging.

The product proved deceptive in other areas – the tray icon, which looked like a marker for the on-access scanner, was in fact a shortcut to the whole program. This 'feature' is not



unique to *CAV*, but it caused initial confusion. In another common flaw, the progress bar bore no resemblance to reality in the on-demand scans, and was far too pessimistic. In terms of stability, this product was not the worst offender, but it certainly managed to distress Explorer into a comatose state on more than one occasion.

CAV lacked a proper silent mode for its on-access scanner. Initially, we thought its insistence on popping system modal dialog boxes and freezing the machine until a key was pressed and released would have it register a 'not tested', at least on-access against the Polymorphic test-set (we have some respect for our keyboards!). Similar Registry tweaks as were found to work around the same issue with the *Data Fellows* product (see below), also worked with *CAV*, allowing full testing.

Cybec VET v9.70

ItW Boot	96.6%	Macro	95.0%
ItW File	100.0%	Macro on-access	95.0%
ItW File on-access	100.0%	Polymorphic	99.1%
ItW Overall	98.8%	Standard	99.3%

VET has had something of a facelift. The smart new packaging projects a more up-market image, and there is a clear effort to incorporate this throughout the product, with new program icons, splash screens and the like all blending with the new look. Initial attempts to configure the on-access component to scan boot sectors seemed doomed to failure. Enabling this option (which was supposedly enabled after installation) and rebooting (it requires the loading of a static VxD), repeatedly produced the rather puzzling message on the program's configuration screen that the option was enabled and would be activated following the next restart.

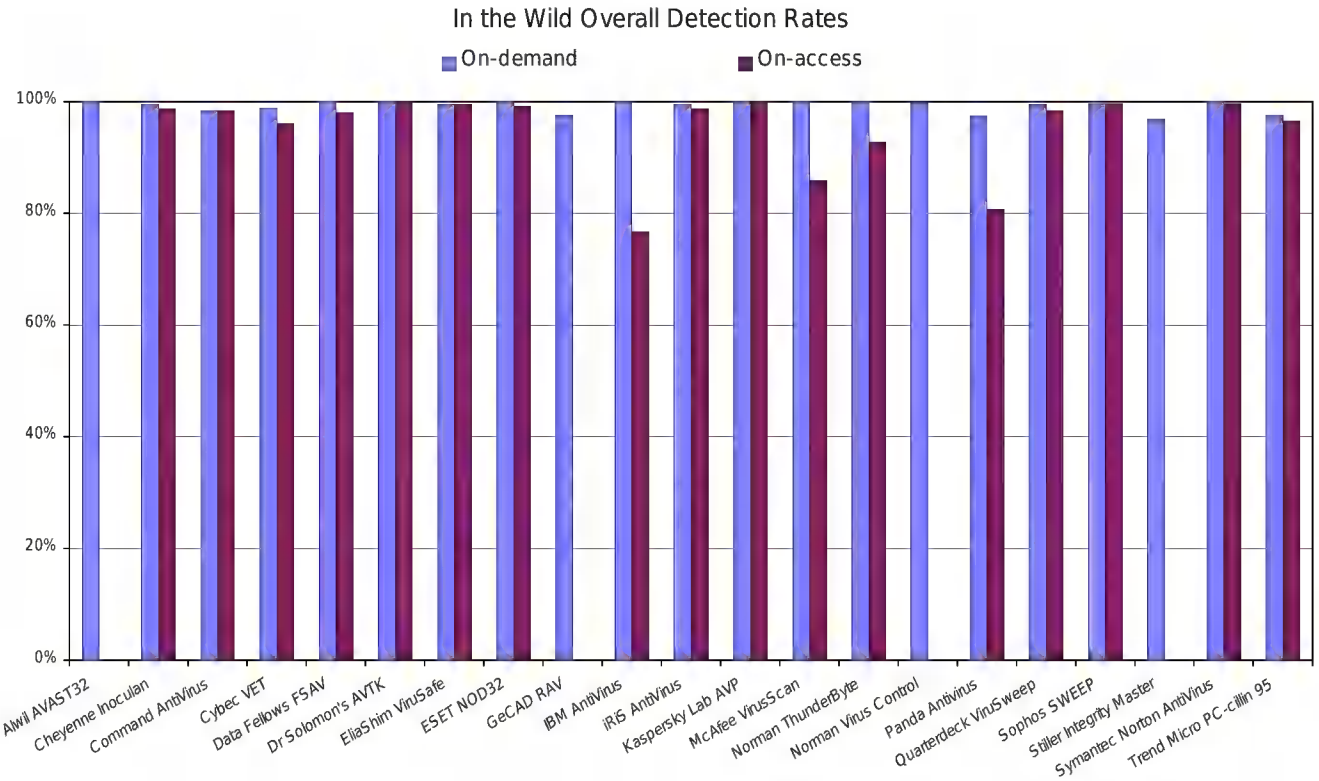
After several discussions with *Cybec's* technical staff, the required VxD was found where it should be and the Registry settings were confirmed as correct. *VB* staff noticed however, that the VxD deposited by the installation process consisted of approximately 17 KB of null characters. The offending item having been replaced and the machine restarted, all came right.

Another bug discovered during testing was that whenever a log file was directed outside the default *VET* directory by typing the full path into the provided entry field, this path would be modified by prepending C:\VET, resulting in several invalid paths (and, we suspect) some of the instability we saw earlier in our attempts to test the product. Using the browse button to specify an alternative path to the log file or closing *VET*, editing the associated Registry setting and restarting the machine 'fixed' this problem.

Cybec is certainly unique among anti-virus developers in offering health care tips for aardvarks in its manuals!

Data Fellows F-Secure Anti-Virus v4.0

ItW Boot	100.0%	Macro	99.3%
ItW File	100.0%	Macro on-access	93.6%
ItW File on-access	97.0%	Polymorphic	99.1%
ItW Overall	100.0%	Standard	100.0%



This is the first time that a multi-engined version of *F-Secure* has featured in a *Virus Bulletin* review, comparative or otherwise. The new product has improved detection over its forerunner and garnered a VB 100% award for its efforts against the In the Wild test-sets. In a previous *Virus Bulletin* test of *F-Secure's* forerunner, the product had some minor stability problems. It seems the subsequent addition of the second engine may have compounded this, although the use of the *AVP* engine is responsible for the significant improvement in detection. That said, the difficulty here is not so much finding problems, as deciding where to start.

Fortunately, as the developers provided an invalid icon offset in the AUTORUN.INF, this allows us to start at the very beginning. This aesthetic bug means that when the CD-ROM is in the drive, Explorer displays an icon usually used with files having no associated application. Not an inspiringly professional look, and this was not a gold CD.

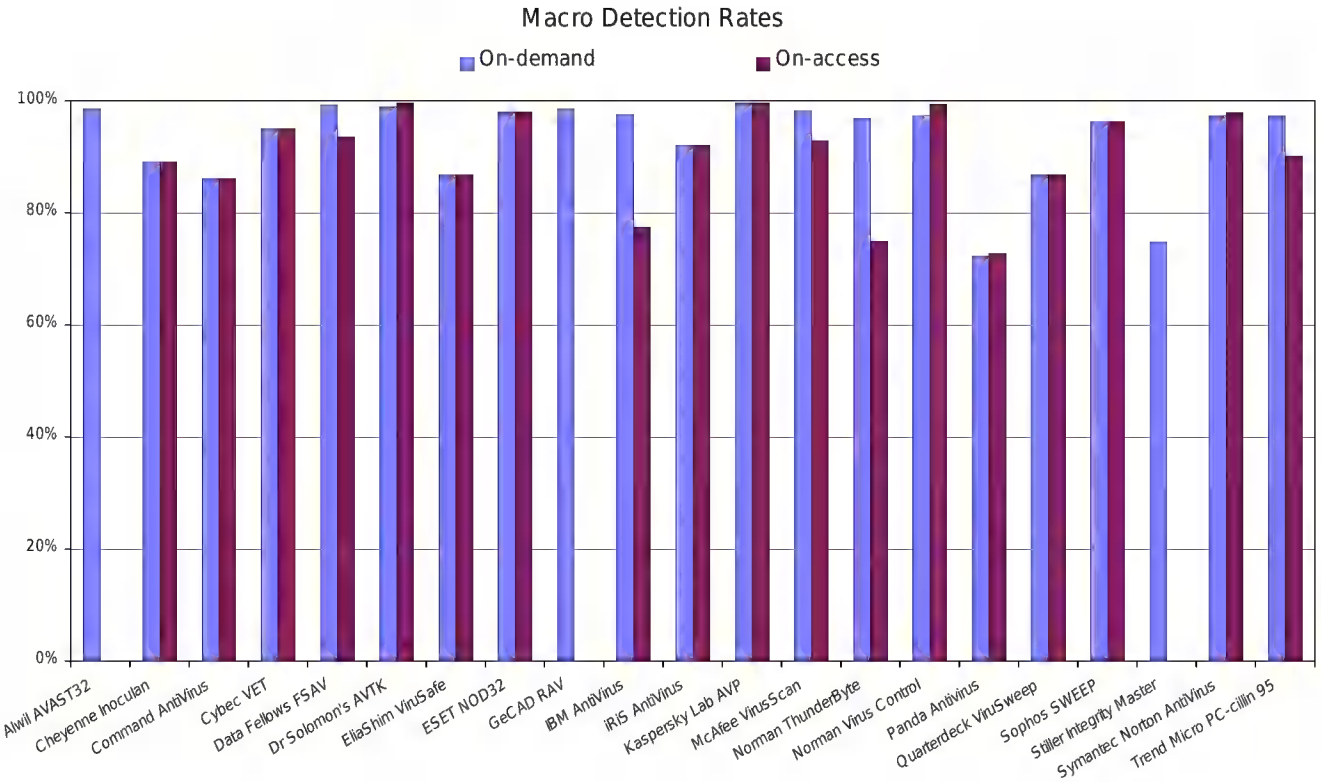
The on-demand scanner was the first tested, and this crashed with great gusto when presented with any significant number of objects to scan. It also proved impossible to scan single files, or indeed to scan more than one branch of a directory tree at one time, though this was due to poor design rather than any errors in the underlying code. One possible cause of the stability problems might be the gargantuan report files, with the two engines each having their say in the case of each file. Entertainingly, this results not only in the detection of more viruses than there are files, but also in the impossibility of knowing at first glance how many files were considered infected. Oh joy.

Related to the design limitation of not being able to scan more than one tree at a time is the fact that there is no browse button on the location to scan field. This omission means that if attempting to scan partial trees, rather than whole drives, one has to type the full path correctly. This should not be a problem, but *F-Secure* does not warn you if an invalid path is entered, and replaces the setting with a weird, semi-random (and still usually invalid) path consisting of some of what was entered and some sub-strings from previous settings.

When scanning directories which did not exist, *F-Secure* performed some madcap antics, and scanned seemingly random paths. As it appeared the log file was not written until scanning ended, the general instability of the program meant that obtaining log files was a hit and miss affair.

So, on to the on-access scanner, which refused to implement one of its options at all. The scanner, without fail, reset itself from merely reporting infections to requiring confirmation and thus a keystroke or mouse click was needed for each virus found. This difficulty was compounded by there being two possible locations to input on-access options, which nevertheless did not necessarily contain the same settings. Unattended testing of the on-access scanner only became possible following discussions with *Data Fellows* technical staff and the manual resetting of some undocumented Registry entries.

The boot sector tests were less fraught affairs. The double declaration of infection continued as an irritation, except in the case of ABCD which was only detected once.



Dr Solomon's AVTK v7.81

ItW Boot	100.0%	Macro	99.0%
ItW File	100.0%	Macro on-access	99.7%
ItW File on-access	100.0%	Polymorphic	100.0%
ItW Overall	100.0%	Standard	100.0%

The *Anti-Virus Toolkit* is beginning to look rather old-fashioned and lacking in options compared to some of the other products on show this month, and had more than its usual quota of problems in this review. However, despite this, it still obtained a VB 100% award.

The on-access scanner was at the root of several problems, insisting upon a reboot at every change of options. Whilst not entirely unexpected, this seems a little too much when the only option changed is the state of report file logging. This component is surely implicated in the problems seen in the on-access boot sector tests, where instability was the order of the day. On-access detection resulted in a notification of infection, followed by a dialog box, apparently of the *Toolkit's* devising. If the diskette was removed from the drive at this point and the retry option chosen, a system hang ensued.

EliaShim ViruSafe 95 v2.6

ItW Boot	98.9%	Macro	86.9%
ItW File	99.9%	Macro on-access	86.9%
ItW File on-access	99.9%	Polymorphic	95.4%
ItW Overall	99.5%	Standard	100.0%

A product displaying no stability problems at all was a great pleasure in this comparative. The multilingual nature of *eSafe Protect* is outdone by this, its sister product, which boasts eight languages to choose from, presumably a number set to increase in future.

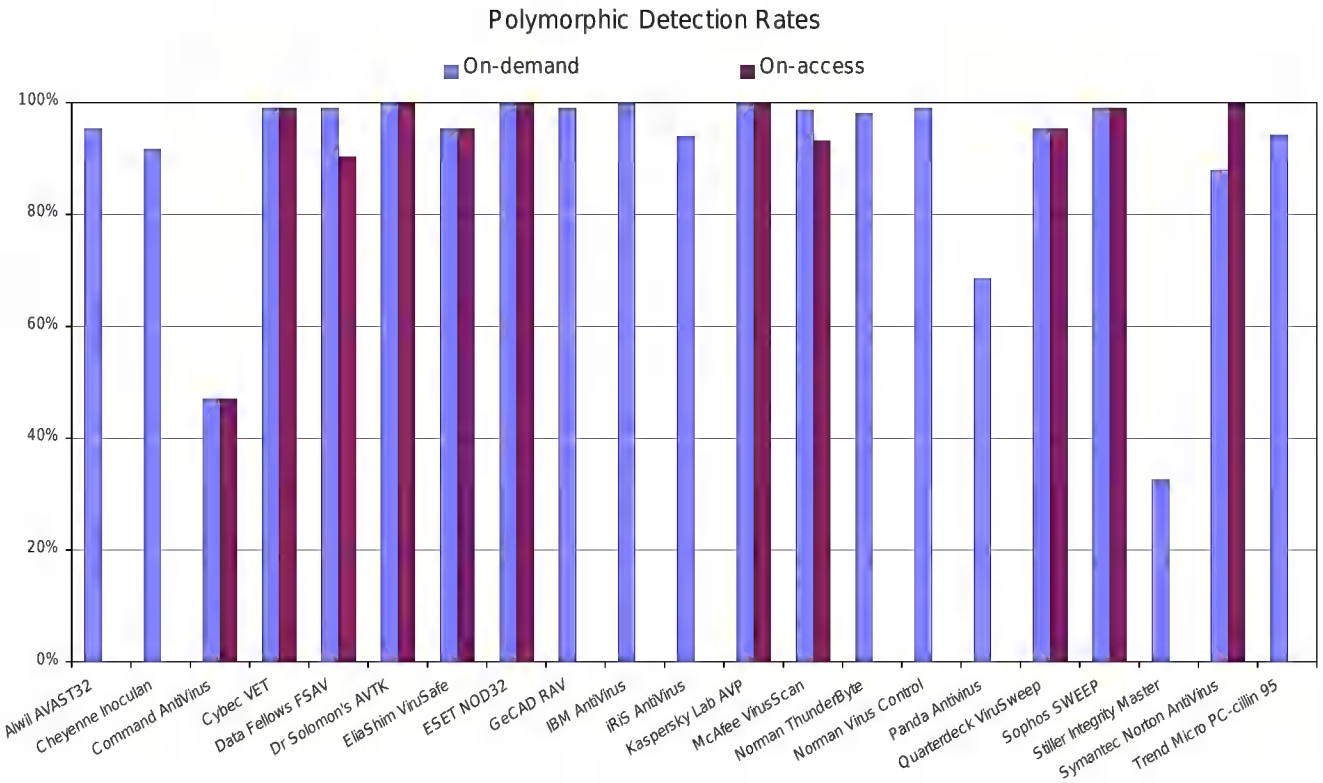
The default scanning configuration installs not only a DOS mode TSR, but also a pre-*Windows* DOS TSR. Again, similar to *eSafe Protect*, there exists an option for a rescue disk, though this is far better documented in the *ViruSafe* manual than in the former product.

Detection results are much on a par with its performance in recent comparatives. Although the *ViruSafe* engine is at the heart of *Quarterdeck's* new *ViruSweep* (see below) – obtaining exactly the same detection in these tests – it seems unlikely that the stability problems with the latter product are due to the *ViruSafe* engine code.

ESET NOD32 v1.00

ItW Boot	100.0%	Macro	98.1%
ItW File	100.0%	Macro on-access	98.1%
ItW File on-access	100.0%	Polymorphic	100.0%
ItW Overall	100.0%	Standard	100.0%

ESET has produced all-new graphics for their *Windows 95* product, though thankfully not at the expense of all-new stability problems. Better yet, detection has been boosted to VB 100% levels in the In the Wild test-set and were tantalizingly close to a clean sweep.



Perhaps not surprisingly, boot sector testing is the area where problems can be found. There were problems for *NOD32* in detecting that disk changes had occurred, leading to very inconsistent detection if the same infected diskette was presented over and over.

On-demand scanning, however, is particularly pleasant to perform, with a full implementation of shortcut keys combined with the holding of focus on those buttons most convenient for scanning a pile of diskettes. The 'directory path a:\ is not valid' messages triggered by diskettes with 'strange' BPBs did not disrupt this convenience, which was topped by the full on-demand detection of the viruses in the Boot Sector test-set. Those same samples prevented *NOD32* from achieving 100% on-access boot detection.

GeCAD RAV v5.22

ItW Boot	97.7%	Macro	98.7%
ItW File	97.5%	Macro on-access	n/a
ItW File on-access	n/a	Polymorphic	99.0%
ItW Overall	97.6%	Standard	96.7%

The Romanian contingent of this comparative proved far more stable than some of its big name cousins, with only false positives and the lack of on-access scanning as notable concerns. The performance is improving compared to recent outings in *VB* comparatives. The setup provided the only anxious moments, with the program warning that a certain DLL needed to be updated. It is peculiar that, although not mentioned as available, the DLL in question is on the DOS scanner disk supplied with the product.

IBM AntiVirus v3.02bc

ItW Boot	100.0%	Macro	97.6%
ItW File	100.0%	Macro on-access	77.4%
ItW File on-access	79.0%	Polymorphic	100.0%
ItW Overall	100.0%	Standard	100.0%

IBM's product proved trickily unstable in the on-demand file tests, which were prone to lock ups when scanning any sizeable number of files whilst logging. The convoluted method in which these log files must be confirmed as to action, in as many as a dozen passes, was not a little distressing.

Worse was to come in the on-demand boot sector scan, where although no viruses were missed, the process of confirming actions took four mouse clicks to perform for each virus. On-access, the boot sector viruses were detected poorly, and some way through testing the dialog box became hidden behind Explorer and was replaced by a blue screen alert. This alert, however, took some five seconds or more to appear and made no friends at all.

iRiS AntiVirus v22.06

ItW Boot	98.9%	Macro	92.1%
ItW File	99.9%	Macro on-access	92.1%
ItW File on-access	99.9%	Polymorphic	94.0%
ItW Overall	99.5%	Standard	100.0%

As stable as a sandcastle submerged at high tide, the degree to which quality assurance has been applied to this product would appear to be negligible. Anti-virus software which

cannot scan a clean *Windows* directory successfully is beyond this reviewer's comprehension. Despite having a pretty interface, all was lost by the contortions required to perform any successful action, though admittedly some of the crashes did produce impressive visual pyrotechnics. The clean scan crashed, a scan of C: drive crashed – the contents being only *Windows 95* and *iRiSAV* itself, a total of 72 MB. Still, *VB* persevered. Experimenting with the use of the sig files (provided with an older and more stable front end) failed to aid matters, as the two were incompatible.

The boot sector tests too, proved far from ideal. On-demand scanning reproducibly failed to detect infections at the first attempt, though a second attempt would often make *iRiSAV* aware that a problem existed. This was highlighted by the virus Baboon – detected once during fifteen accesses.

Kaspersky Lab AVP v3.0.119

ItW Boot	100.0%	Macro	99.7%
ItW File	100.0%	Macro on-access	99.7%
ItW File on-access	100.0%	Polymorphic	100.0%
ItW Overall	100.0%	Standard	100.0%

With a review of this very same product elsewhere in *VB* this month, there is little but a summary that can be added to the words there. *AVP* behaves as it should under the test conditions, and easily detects sufficient viruses to qualify for a VB 100%. *Kaspersky Lab* will no doubt be aiming for complete detection in all categories in the next comparitive, with a good chance of success.

McAfee VirusScan v3.15.3103

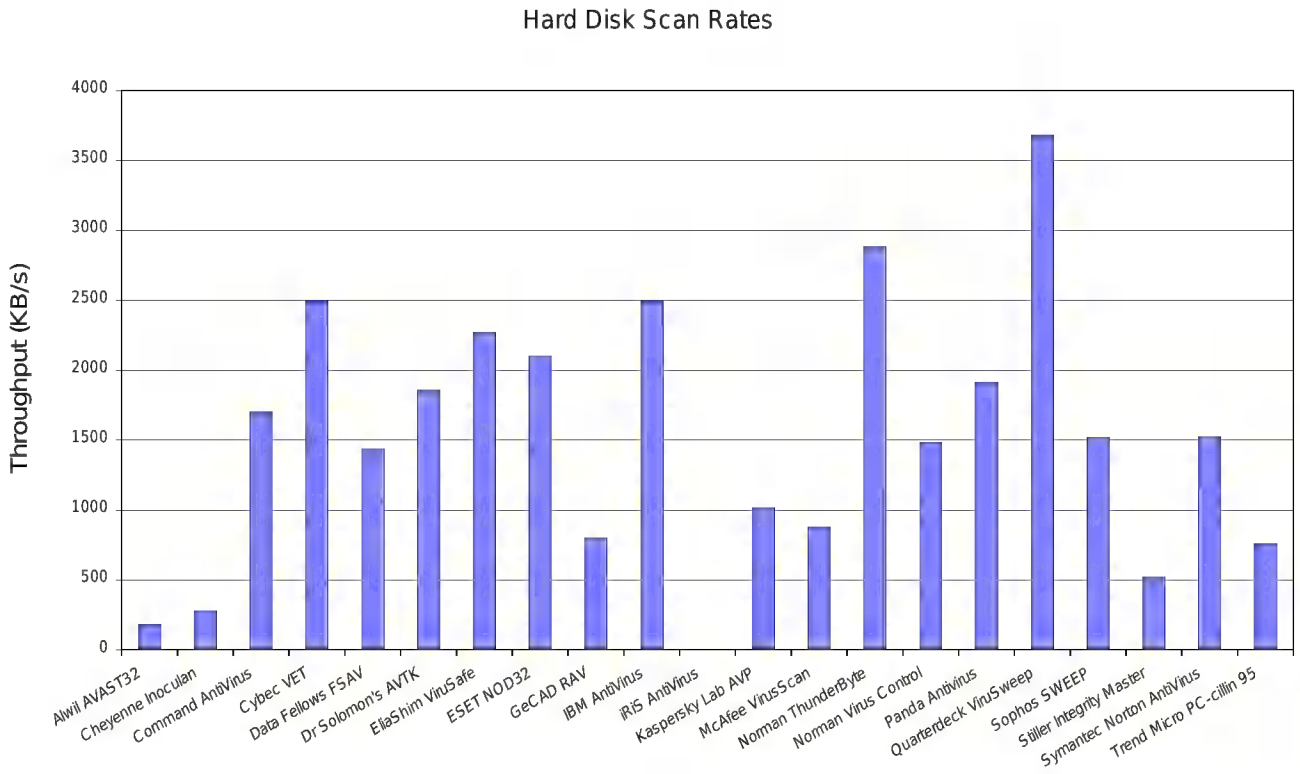
ItW Boot	100.0%	Macro	98.3%
ItW File	100.0%	Macro on-access	92.9%
ItW File on-access	100.0%	Polymorphic	98.7%
ItW Overall	100.0%	Standard	98.8%

The problems encountered by *VirusScan* in the last boot tests seem to have been swiftly overcome, and on-demand scanning of boot sector diskettes was comprehensive, though not always at the first attempt. On-access, however, boot sector viruses proved elusive, with over one third remaining undetected. The *NT* stability problems seemed to a great degree banished.

Norman ThunderByte AntiVirus v8.05

ItW Boot	100.0%	Macro	97.0%
ItW File	100.0%	Macro on-access	75.0%
ItW File on-access	90.8%	Polymorphic	98.1%
ItW Overall	100.0%	Standard	98.1%

TBAV is stable, and its only faults lie in areas irrelevant to the average user, but still caused some problems in the review process. More relevant is the time taken to install *TBAV*. The installation process begins by a scan of all local drives, followed by a checksum of those drives. On the *VB* test machine with a moderately laden drive this two pass process took over an hour. This, however, is unlikely to be a problem except on the busiest or most vital of workstations.



Similarly, the lack of a quiet mode on the active i/o monitor made testing problematic. It was noteworthy that the production of a modal blue screen or modal information box seemed to occur almost completely at random.

These niggles are slight – *TBAV* was the speediest product to check multiple disks, as it was placed in a mode where the A: drive was constantly accessed, and scans any disk inserted. As new disks are always scanned, this makes scanning a matter where no keyboard input is required.

Norman Virus Control v4.35.4.6

ItW Boot	100.0%	Macro	97.4%
ItW File	99.7%	Macro on-access	99.4%
ItW File on-access	n/a	Polymorphic	99.0%
ItW Overall	99.8%	Standard	99.7%

Another program with admirable stability, though the usual comments about the on-access component still apply. The *Norman* on-access system consists of a behaviour blocker (operational on file execution) and Cats Claw, which screens for macro viruses. The former of these proved impossible to test against anything but the Boot Sector test-set, where it discovered all but five samples, declaring the others to have been detected 'by statistical tests'.

The file scan options were tested for stability more than for overhead ratings and showed no problems on this front. Of note was the behaviour blocker in 'strict' mode, which considered even the simple copying of executables to be a possible sign of viral infection.

On-demand in the boot sector tests a score of 100% detection was achieved with no glitches or irritations.

Panda Antivirus v5.0

ItW Boot	87.0%	Macro	72.4%
ItW File	96.2%	Macro on-access	72.7%
ItW File on-access	87.5%	Polymorphic	68.6%
ItW Overall	97.5%	Standard	80.8%

Another first-time appearance, this Spanish product should not be confused with the *Dr Panda Utilities* from (distant) past *Virus Bulletins*. The readme file contains the usual hyperbole (in this case, somewhat more outrageous). A built-in list of 38 potential target file extensions seemed a little paranoid (although the default 'active' extensions from this list is little different from most other products).

Interestingly, in the boot sector virus tests, *Panda* pro-claimed merrily that there were two viruses present on each of five of the single sample diskettes. The Jumper.B sample topped this, however, apparently being host to three infected boot sectors. Most of these multiple reports were common aliases for the virus actually present, but if this is *Panda's* mechanism for conveying that information, this should be made clearer. If not, it would seem that some duplicate virus signatures are present in *Panda's* library.

As the on-access scanner had no discernible silent mode, the on-access tests were only run through the In the Wild Boot, File, Macro and Standard test-sets, by which time the tester's wrists were glad of a change of scene.

Quarterdeck ViruSweep v1.00

ItW Boot	98.9%	Macro	86.9%
ItW File	99.9%	Macro on-access	86.9%
ItW File on-access	99.9%	Polymorphic	95.4%
ItW Overall	99.5%	Standard	100.0%

A new product for review, which is clearly having a few teething troubles. Rather unusually for a *Windows 95*-only product, the CD-ROM does not have an autorun feature. Upon starting the installation process manually, an error dialog popped open, due to the linking of a DLL to a non-existent OLE file. Things were not looking good at this point, and indeed, this did not bode well for the testing process itself.

On rebooting the system after installation, the QSM (presumably the Quarterdeck Service Manager) produced errors due to illegal operations. This fault was not fixed following installation of the supplied update, so QSM was removed from the Startup group on the test machine. An annoying quirk during installation was that, despite disabling the 'make a rescue disk' option early on, this effort seemed to have been ignored later in the process, when a prompt appeared asking if one should be made.

Peculiarity was the order of the day during the on-access boot sector virus tests. Re-testing of those viruses not detected produced, on occasion, a report of a completely different virus detection, although the virus detected was (usually) that from the immediately previous diskette. This was followed by a selection of other possible infections being logged, and eventually a blue screen was the result.

On-demand boot sector detection was also not without problems. The VxD screen appeared some, yet not all, of the time – an oddity that initially seemed related to some of the scanner's settings, but reappeared after a confusing spurt of reliability and then could not be vanquished.

Overhead tests further proved the lack of consistency in *ViruSweep*, since XCOPY was labelled at random as showing virus-like behaviour – 'ViruSweep Important Interrupts have been changed by command.com' being the rather strange warning. This annoyance was removed by deactivation of interrupt checking.

Sophos SWEEP v3.07

ItW Boot	100.0%	Macro	96.4%
ItW File	99.4%	Macro on-access	96.4%
ItW File on-access	99.4%	Polymorphic	99.0%
ItW Overall	99.6%	Standard	99.7%

Another of the non-crashing achievers of this comparative, we are back to minor niggles with *SWEEP*. The on-access scanner, *InterCheck*, is proclaimed in the manual to be non-removable under *Windows 95*, but this proved to be possible using the very *NT* configuration commands the manual specifically declared were unsupported under *Windows 95*. On the other hand, the 'deny access' option of this scanner did indeed do just that during the In the Wild Boot tests, where all viruses were detected. Were Explorer human, it would probably have been puzzled by the number of apparently unformatted diskettes it was seeing.

On-demand, the boot sector viruses were all discovered, although there was a peculiarity in the change of focus after virus detection. Combined with the inability to use Alt-F to produce a file menu, this slowed the rate of scanning diskettes considerably.

Stiller Research Integrity Master v4.01

ItW Boot	97.7%	Macro	74.8%
ItW File	96.6%	Macro on-access	n/a
ItW File on-access	n/a	Polymorphic	32.7%
ItW Overall	97.0%	Standard	85.6%

Stiller Research's product is a little out of place in this review, and suffers a fair amount as a result. The primary protection method offered by *Integrity Master* is that of checksumming, and the detection of illicit changes to files – whether viral in origin or the actions of unauthorized personnel. As a result, the security and checksumming portions of the program are considered more important than the scanning portions. *Stiller Research* goes so far as to suggest that another scanner be used in conjunction with *Integrity Master*. The theory behind this is that a scanner will pick up known viruses, while *Integrity Master* prevents data damage caused by any that slip through the net.

Sumi AspVIRin AntiVirus

The developers of this Romanian product were keen to introduce it to *Virus Bulletin* testing. The supplied product installed quickly and apparently efficiently, but all attempts to run the main executable failed with a series of page faults. The trial version was downloaded from their web site, but it performed in exactly the same way. Installing Eastern European language support on the test machine did not resolve the matter either. Email to the developers went unanswered, so we abandoned trying to test the product.

Symantec Norton AntiVirus v4.04

ItW Boot	100.0%	Macro	97.4%
ItW File	100.0%	Macro on-access	98.0%
ItW File on-access	100.0%	Polymorphic	88.0%
ItW Overall	100.0%	Standard	99.1%

Yet another program where stability *and* predictability were to be found, though here it was fairly localized. After by far the prettiest of the splash screens (involving spaceships, sound effects and a rolling graphics show), the standard CD offered the option to watch four videos, ranging in content

and style from mildly informative to cheesy. If these are used as a guide, the *Symantec* corporate image is that of a sideburnless Elvis in a fetching gold lamé suit.

Unlike so many other products, most scanning was performed without distress, though boot sectors proved something of a fly in the ointment. On-access scanning of floppies was wont to hang the test machines irretrievably should the diskette be removed too soon. In this context, 'too soon' includes a period of time after which all visible and audible disk access had finished! When a virus was detected, *Norton Antivirus* proclaimed that access had been denied, yet after a short period of time Explorer was apparently allowed enough access to decide that the sample diskettes were devoid of files, rather than not formatted. Despite these peculiarities, the only boot sector virus missed during on-access testing was Moloch.

On-demand boot sector tests produced no misses, though strange events occurred when faced with Michelangelo.A, Michelangelo.S, and MISiS. These samples have strange BPBs (for a diskette in a high-density 3.5-inch drive), which triggered the message 'Unable to access drive A:. The drive is locked with a disk utility. Scan again later when the disk is no longer locked'. Contrary to general intuition, at this point selecting 'skip disk' allowed *Norton Antivirus* to detect the infections upon these media.

The lack of a 'proper' silent mode made on-access testing slow, if not interesting.

Trend Micro PC-cillin 95 v3.0

ItW Boot	95.4%	Macro	97.4%
ItW File	98.7%	Macro on-access	90.2%
ItW File on-access	97.2%	Polymorphic	94.2%
ItW Overall	97.6%	Standard	98.5%

The product *Trend* submitted for review sat comfortably with the illustrious company inhabiting the 'non-functional' end of this comparative review. Things started nicely, as while installing the application, no problems were apparent. However, once installed almost any attempt to use any part of the product resulted in a message to the effect that this was an 'unsupported option'.

As scanning was amongst these unsupported options the future looked far from rosy. For the purposes of having at least some test results, an evaluation copy of *PC-cillin* was downloaded from the WWW and the signature file supplied with the review copy implanted into the evaluation product's installation. The result was a program with some limitations in functionality, though none of these related to tested actions (several of the Internet-related functions – including on-line updating and registration – and the disinfection wizards were not available).

Even after these steps had been taken there were still gripes aplenty to be addressed. As an *entré*, the button to start an on-demand scan was without an accelerator key. This is immensely frustrating when having to scan more than half a dozen or so diskettes. In an attempt to ease testing the 87 diskettes in the Boot test-set, the focus was tabbed to this button in the hope that a cycle of keypresses could be discovered to speed the testing. However, once this button was visually selected, pressing the Enter key caused the program to terminate completely. On-demand boot testing was not a pretty experience...

Having devised a process that seemed to work, boot sector viruses were not the most impressively dealt with. Despite having *ICSA* and *Secure Computing* certifications that the product detects all In the Wild viruses, a handful of misses in the ItW Boot tests seems to be all but expected in *Virus Bulletin* tests – it would be a pity if this had been fixed in the version sent for testing. Somewhat surprisingly, the option 'deny access to infected files and continue' seems to have been taken too literally – boot sectors are not, technically, files and thus Explorer was not prevented access to the rest of boot sector virus-infected diskettes. Added to this was an idiosyncratic method of detecting disk changes, which made more mistakes than it should have.

On access scanning also proved problematic when reasonably large numbers of files were passed through *PC-cillin's* gaze. The attemps to test on-access detection of the whole *Virus Bulletin* test set resulted in reliable crashing of the system, and more disturbingly this was reproduced when merely perusing an uninfected installation of *Windows 95*.

Conclusion

While congratulations are due to those nine products which acheived VB 100% awards, this is not to say that they were by any means perfect. More than one of these exhibited such grievous imperfections in either user interface or general stability as to be barely serviceable. On the other hand, some products, despite being a pleasure to use, displayed significant faults in their detection capabilities.

As mentioned at the beginning of the review, brute force detection is not the 'be all and end all' of an anti-virus product. If only to maintain the sanity of testers, it is to be hoped that quality assurance may become a more prominent part of product development.

Technical Details

Test Environment: Three 166 MHz Pentium-MMX workstations with 64 MB of RAM, 4 GB hard disk, CD-ROM drive and a 3.5-inch floppy, running *Windows NT v4.0 (SP3)*. The workstations could be rebuilt from disk images and the test-sets were held in a read-only directory on the server. All timed tests were run on one workstation.

Speed and Overhead Test-sets: Clean Hard Disk: 5500 COM and EXE files, occupying 546,932,175 bytes, copied from CD-ROM to hard disk.

Virus Test-sets: Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/Win95/199805/test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.

PRODUCT REVIEW 1

Intel LANDesk Virus Protect v5

LANDesk Virus Protect (*LDVP*) is normally presented as an enterprise solution – a product providing virus protection to your servers and desktops. Specifically, it provides *NT* and *NetWare* server scanners, and desktop scanners for DOS and *Windows 3.1x*, *95* and *NT* workstations. Server-only and client-only licences are also available. This review focuses on the *NetWare* server component.

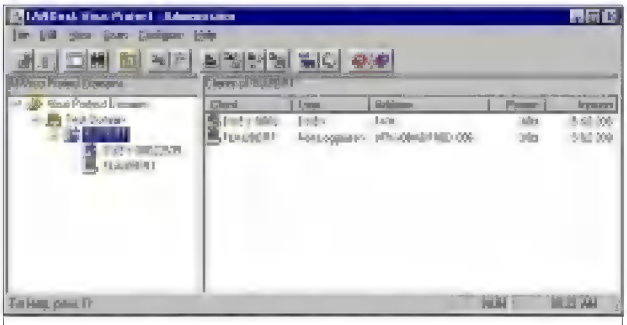
LDVP is licensed on a per-server basis. The licence with the review copy covered a single server and all users who connect to it. *Intel* provides five- and twenty-server bundles and the manual states that bulk licence agreements can be arranged. Twenty-server licences require one serial number per twenty installed servers, but there is also mention of a Gold Disk contract, allowing purchasers of fifty or more server licences the option of a single serial number.

The licence covers installation on one or other of the supported server operating systems, but not both concurrently. As is fairly standard these days, the client licence extends to laptop or home computers owned by the user of a computer covered by the network licence. Non-networked company laptops require separate client licences.

Presentation and Documentation

The product was packaged in a pleasantly designed box, albeit of rather too light weight construction, judging by its crushed countenance on arrival. The artwork is clearly and simply laid out and the outlandish claims seen on the packaging of some vendors do not feature here, thankfully. The back of the box is given over to a brief description of *LDVP's* features and a clear listing of minimum system requirements for the various supported platforms.

The box divulged a customer support reference card (distinctly North American in outlook), a separate Quick Start card for the server and client software (copies of the latter can be produced from the CD), an Administration Guide and jewel-cased CD. The CD turned out to be a hand-labelled CD-R disk claiming to be the release code of v5.02. In one sense I hope it was not the release code, as the AUTORUN.INF file contained an error such that *Windows* Explorer displayed the icon more usually associated with an unknown file type against the CD drive when the *LDVP* CD-ROM was in the drive. Also included were the obligatory licence agreement and mail-back registration cards. Registration may also be completed via fax or the WWW.



With more than a passing similarity to the *Windows* Explorer, *LDVP's* Administrator should be easily mastered.

The Administration Guide is easily followed. It runs through a description of the product – how it works, planning for and performing installation and rollout, centralized administration and advanced configuration issues. This is a comfortable progression for a new user and the logical layout should not distract an *LDVP* 'veteran'.

That said, there are some small inconsistencies, both within the manual and between the manual, software and on-line help. For example, there is noticeable disagreement as to what types of archives are scanned when the compressed files option is selected. The manual's index is neither scanty nor prodigious, but I seldom found myself referring to it. The organization of the content generally guides you to the correct place when you need to refer to material beyond the scope of the current section.

Straddling the divide between providing printed documentation and only an electronic form, *Intel* seems to have incorporated the manual into the on-line help files. This should keep both page-thumbers and mouse-jockeys happy.

Installation

As is increasingly common with server products, *LDVP* provides an administration program that runs separately from the scanner. In *LDVP's* case, this can control 'domains' of *LDVP*-protected servers and workstations. The *LDVP* Administrator only runs on Win32 machines, as does the installation program for the server product.

On running the setup program you are presented with the choice of reading the release notes or running a client or server installation. Choosing the latter, you select from install, update and uninstall options. Selecting install and agreeing to the licence terms resulted in the offer of browsing the on-line help coverage of system planning. Having read this material in the printed manual, I braved the Next button, to be presented with check-box selections to enable installation of the three main components of the *LDVP* server software – the Administrator program, the server scanner and the Alert Management System (AMS^2).

Having selected all three (the default), I was presented with a list of *NetWare* and *NT* servers on the network. Adding the target server to the destination server list, I was asked

for login details, as I was not logged into the selected server. Logging into an account with insufficient privileges (Supervisor or equivalent is required) resulted in an 'access denied' error, and did not provide the means of resolution.

Logging in as Supervisor (in Explorer), the next task was to enter the 14-digit licence number or choose the 45-day 'test drive' option. The chance to change the installation path on the selected servers was offered, and I was then asked to place the target server in a Virus Protect domain.

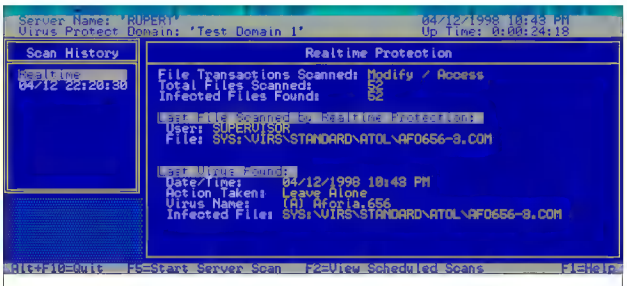
An option to start the server software automatically followed – if selected, VPSTART.NCF is called at the end of the server's AUTOEXEC.NCF. If this option is declined, you must start the *LDVP* modules following a server restart by calling that command file manually. Regardless of the option chosen here however, the scanner must be loaded manually following the completion of installation.

There followed a request to select the target directory for the Administrator program on the installation workstation, a warning about manually starting the scanner on the server, guidance on starting the Administrator program under the operating systems that support it, and a reminder of the default domain password (as a new domain had been created for this test). Reaching the dialog with the prized 'Finish' button, I was reminded of the various options for installing the client software. After the progress bar had disappeared, the virtually obligatory readme file was offered for viewing, as was the similarly ubiquitous suggestion of a post-install restart.

In Use

There is not much to see on the server. The main *LDVP* console displays a list of currently running and recent scanner tasks. You can toggle between them and check their status. An immediate server scan can be started from the console and scheduled scans previewed. The scanner can be unloaded, but only from its console screen and only after entering the password for its security domain. Obviously, most of the action occurs away from the server at the *LDVP* Administrator machine.

From the latter machine, server scanning options are much the same (though separately configured) for manual scans and realtime protection. The differences are that manual scans can be configured as to which drives and folders to scan and to be aware of *NetWare* compressed files, whereas real-time scanning offers choices of scanning on file access and/or modification, whether to monitor for virus-like behaviour and whether to scan floppy and CD-ROM drives. Scheduled scans have the same options as manual scans.



Not having to deal with configuration issues, *LDVP's* server console is a fairly spartan affair.

Configuration options common to all scan types are: a choice between scanning all files or just those with certain extensions (this is the default, and the pre-configured extensions are BIN, COM, DLL, DOC, DOT, EXE, SYS, XLS and XLT); scanning inside archive files; excluding selected folders and/or files; excluding detection of selected viruses; the separate actions to take on detection of macro and non-macro viruses; the display and content of virus detection warnings, and the quarantine folder to use with the 'move infected file' action.

On detection of a virus, the actions available for all scan types are move, rename, delete, leave alone, and clean. If any action other than leave alone is selected, a secondary action can be chosen, should the first fail. These options are set separately for macro and non-macro viruses.

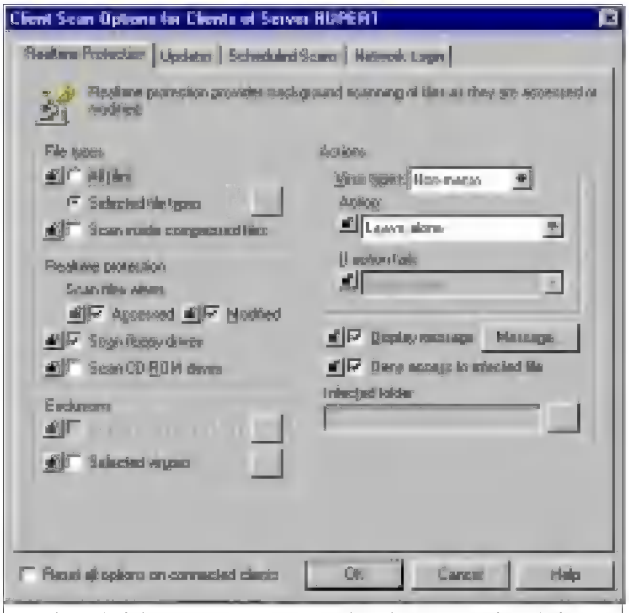
Scheduled scans can be set to run daily (you choose the time), weekly (choose the day and time) and monthly (choose date and time). Scheduled scan configurations need not be activated, although only those which are activated are shown on the server console display.

The Administrator program can start an immediate scan of the server using any schedule profile, whether activated or not. There are no options to prevent a scheduled scan running for more than a given length of time nor to run an external command upon completion of the scan.

Administration and Reporting

The *LDVP* Administrator has a look and feel akin to the *Windows* Explorer. Right-clicking a domain, server or workstation brings up a context menu of the more commonly performed actions for that type of object. There are options to force on-demand scans of any protected server or Win32 workstation. Domains can be 'swept', in which case all servers and *Windows* workstations (including 16-bit clients) in them are scanned. Similarly, servers and all attached *Windows* workstations can be swept. Scan histories of servers and event logs of domains can also be viewed.

The Administrator allows a high degree of control over the scanning options of a domain's workstations. The Administrator's choice of options can be set and 'locked', so workstation users cannot override them. Scheduled workstation scans can also be enforced by the Administrator. Further options force connected workstations to keep their pattern files in synchronization with that on the server and to check for updates and install the client software from server login scripts. Clients normally check for changes to these settings every 300 minutes, but that value can be configured to suit your needs, and you can reset all currently connected clients immediately.



The Administrator can prevent workstation scan options being changed by clicking the locks to the left of the settings.

AMS[2] provides an extensive range of incident reporting options for *LDVP* domains. These include sending alerts via Internet (SMTP) email, SNMP traps, external paging services, workstation message boxes or network broadcasts and loading an NLM.

Virus Detection and Overhead

A manual scan posted the very creditable result of 100% detection on each of the In the Wild File, Standard and Polymorphic test-sets. Identical detection was obtained by the realtime scanner. The only viruses missed in the whole test were the four samples each of the recent macro viruses W97M/AntiSR1.A, W97M/KLA.A, W97M/Wazzu.DG and WM/MortalKombat.A. These viruses were missed by both manual and realtime scans, giving an overall detection rate against the Macro test-set of 98.7%.

To determine the impact of the on-access scanner on the server, two hundred COM and EXE files of 20.6 MB were copied from one server directory to another using *NetWare's* NCOPY. Using NCOPY keeps the data transfer within the server itself, minimizing network effects. Due to the different processes which occur within the server, the tests were run ten times for each setting and an average taken. The test conditions were:

- NLM not loaded. This establishes the baseline time for copying the files on the server.
- NLM loaded; scanning disabled. This tests the impact of the scanner loaded in its quiescent state with no real-time or immediate scan in progress.
- NLM loaded; scan files when modified. This shows the overhead when scanning incoming files.
- NLM loaded; scan files when accessed. This shows the overhead when scanning outgoing files.
- NLM loaded; scan files when modified or accessed. This shows the overhead of having both read and write scans in effect.
- NLM unloaded. This is run after the other tests to check how well the server returns to its former state.

As the results in the product summary box show, there was little difference in overhead between the scan on access and scan on modification options. However, 220% seems a high overhead to pay for virus scanning. In the high paranoia mode with both options enabled, servers with heavy file I/O will really feel the pinch.

Conclusion

Combining good management and alerting features with improved virus detection, this new version of *LANDesk Virus Protect* is likely to keep *Intel's* product in contention with the other leaders in the enterprise anti-virus pack. LDVP's server overhead is definitely in the 'needs looking into' class, but IT control freaks might be hard-pressed to find better client management capabilities.

LANDesk Virus Protect

Overhead of On-access Scanning:

The tests show the time (in seconds) taken to copy 200 executable files (20.6 MB). Each test was repeated ten times, and an average taken.

	Time	Overhead
NLM not loaded	13.6	-
NLM loaded, inactive	14.8	8.8%
— + scan on file modification	43.8	222.1%
— + scan on file access	43.6	220.6%
— + scan on both	61.8	354.4%
NLM unloaded	11.0	6.3%

Technical Details

Product: *Intel LANDesk Virus Protect v5.02.*

Developer: *Intel Corporation (UK) Ltd*, Piper's Way, Swindon, Wiltshire, SN3 1RJ, Tel +44 1793 431155, fax +44 1793 513142.

UK Vendor: *Action Computer Supplies*, 12 Windmill Lane, Southall, Middlesex, UB2 4QD, Tel +44 181 9002566.

Availability: The server NLMs require 2 MB of RAM and 5MB of free disk space (an extra 17 MB of disk space if the client setup images are installed). The Administrator requires a Win32 client with 16 MB of RAM and 10 MB of free disk space.

Version Evaluated: Version 5.02 (Build 208).

Price: Single server licences £300, server plus five client licences £370, plus 25 clients £620 and unlimited clients £930. Contact the vendor for larger site licence pricing.

Hardware Used: Server: *Compaq* Prolinea 590, 80 MB of RAM, 2 GB hard disk, running *NetWare 3.12*. Workstation: One 166 MHz Pentium-MMX workstation with 64 MB RAM, 4 GB hard disk, CD-ROM drive and 3.5-inch floppy drive running *Windows 95 (SP1)*; one *Compaq* DeskPro 466, 16 MB of RAM, 230 MB hard disk, running MS-DOS 6.22 and *Windows 3.1*.

Test-sets: Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/Win95/199805/test_sets.html.

PRODUCT REVIEW 2

AVP v3.0 for Windows 95

AntiViral Toolkit Pro (*AVP*) has a good record of high detection rates. Although this slipped somewhat while development effort was focused on revamping and extending the product line to cover the 'expected' operating systems, *AVP's* performance in recent *Virus Bulletin* comparative reviews shows a healthy recovery.

As reported in last month's issue, the developer's parent corporation, *KAMI Ltd*, recently fragmented into several smaller companies, and *AVP* is now produced by *Kaspersky Lab*. As yet, this division is only reflected in the packaging which, none the less, retains the earlier overall design. The manual makes mention of *KAMI Ltd*, but more of that later. What remains to be seen is whether *AVP* itself has improved or deteriorated.

Packaging and Installation

AVP is supplied in a standard-sized box, containing a licence agreement, a slim (60-page) manual, and the program diskettes. The shipped diskettes were not write-protected, which could cause problems if attempting to set up *AVP* on an infected PC. The disks are contained in a cardboard 'cage' – a variation on the usual envelope – the breaking open of which is considered to be legal acceptance of all the licence terms. Use of the program is limited to within one year of purchase.

The licence itself is fairly typical, apart from Russian being the first language and English the alternative. A Russian influence is also noticeable in the manual, which includes some interestingly creative uses of English. Although the manual is clear in its instructions, it contains information so outdated as to be positively misleading. This is apparent from the very start, as the installation program referred to does not exist!

The installation program is not hard to find as there is only one file on the first installation disk, and its name is an anagram of that mentioned in the manual. The same name is also divulged later, inside the README.TXT file. Unfortunately, that file is only available after the installation procedure is complete, at which point the information has become irrelevant for those souls who rely on this sort of documentary help.

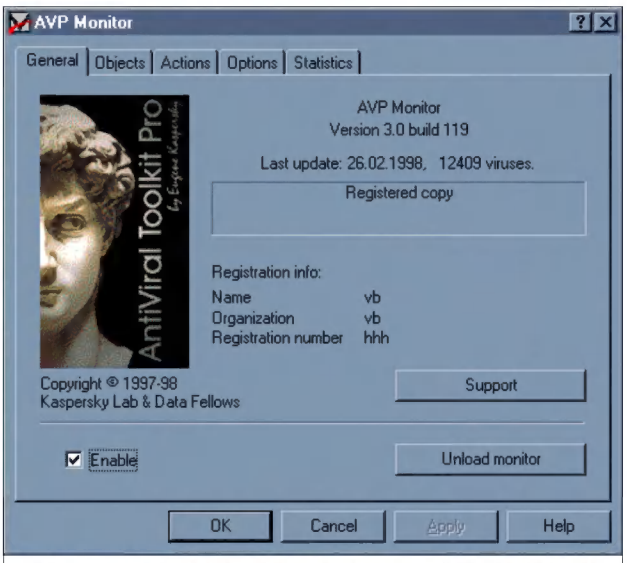
In general, trying to follow the manual's instructions would be especially confusing for the inexperienced user. Furthermore, there is no mention of the on-access scanner, though such a component has now been implemented, and it is automatically activated upon completion of installation. It is hoped that the manual is soon updated to include coverage of such an important component of the product.

Registration is part and parcel of the installation process, though it may be carried out later with the use of a key number. *AVP* may be installed without registration, which, according to the manual, removes the ability to scan inside packed or archived files, disinfect files or to scan remote disks. Strangely enough, the use of a completely bogus key number still seemed to give the option to scan within compressed files and also to disinfect. Once more, a reference to README.TXT was in order.

This file included a different set of exclusions for non-registration – no cure option, no installation from a server and no analysis for unknown viruses. This still failed to explain, however, why the product claimed to be registered when the registration key used was so patently bogus – a situation clearly visible in the *AVP* monitor screen-shot.

Given the problems with the printed manual, the on-line documentation was chosen for reference whenever feasible. This material is not the vast, sprawling epic of some programs. Unfortunately, the more recent nature of the on-access scanner is a problem here, with no on-line help available either, though there is a help button.

Installation being complete, there are three executable programs available: the on-demand scanner, the control panel for the on-access monitor, and UNWISE.EXE. The latter is a standard, albeit intriguingly named, uninstallation utility, and is perhaps best known because its name gives rise to many technical support calls (including those to *Virus Bulletin*). Many who have not struck it before assume it might be some fiendish new virus or Trojan Horse. This is also the first chance to peruse the README.TXT file.



A commonality of design runs through the product. The General tab of the on-access configuration utility, which simply allows enabling and disabling of the active monitor, is shown.

As well as the information mentioned above the readme file contains some useful general and support information, including an exhaustive list of FTP sites where *AVP* is available, a selection of associated BBSs and a sizeable clutch of useful World Wide Web addresses. Snail mail addresses are provided for a list of suppliers and sources of support, encompassing all continents bar Antarctica and South America!

The installation process ran flawlessly on the standard Pentiums used as default machines in the *Virus Bulletin* tests, and the product ran reliably on these with an admirable lack of stability problems. An alternative test machine managed to throw up a reproducible glitch on exiting the main *AVP* component, where despite performing scans with no problems, the termination of the application regularly triggered an invalid page fault. However, with the offer of a free evaluation copy of the product, any stability problems can be spotted early.

On-demand Scanner

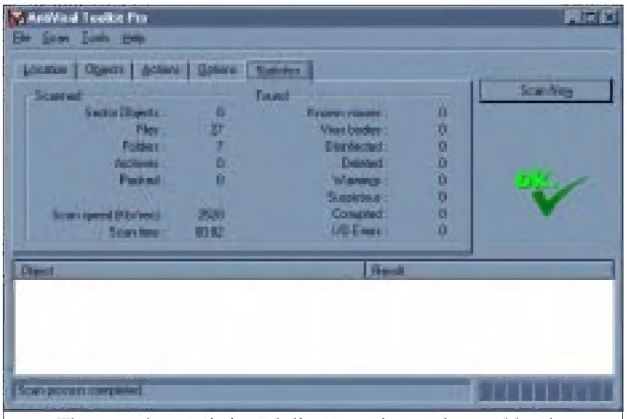
Both the on-demand and on-access modules of *AVP* can be tailored to suit the need of the moment. The on-demand scanner can be configured with respect to 'location' of scan, 'objects' to scan, 'actions' upon detection and miscellaneous 'options'. A final menu gives an overview of scanning 'statistics'. Profiles may be set up and saved, so that commonly used scanner configurations need not be selected at each scan.

The scanning of floppies is designed to make checking multiple disks easy – a task not uniformly pleasant with other products. There was a slightly odd twist to the scans, in that with non-standard formats an option was given to format the supposedly unformatted disk, despite a virus having just been discovered.

At its default setting *AVP* will scan within packed but not archived files and performs a memory and boot sector test as well as scanning typical file types. Scanning of packed files is particularly significant in Russia, where Cruncher, a virus that uses DIET to pack infected files, is prevalent.

Each of the options mentioned above can be selected or deselected at will, using standard *Windows 95* check boxes. The file types checked are as expected, though documents may be skipped in the scan if desired. There are options to scan every file rather than those currently acknowledged as viral vectors and to create an entirely user-defined set of file extensions.

On detection of a virus there is a wide range of possible actions, from the user-transparent log to a report file, through moving the file to a special directory, to automatic deletion or disinfection. Perhaps the most useful option is that which allows you to choose from the list. In the case of 'suspicious' files such as those triggering *AVP's* heuristic detection, there is only one option – transferral to a directory for further study.



The scanning statistics tab lists any viruses detected by the associated scanner – the on-demand one or the Monitor.

There is a range of choices relating to the log file. This normally lists just infected objects, but can also be set to include information on clean files, and extended information on packed files. The log files are straightforward in their presentation.

Although the option exists to turn off sound effects, the program makes use of sounds in such a low-key fashion that only the most fastidious or phonophobic user is likely to disable them. No problems were encountered when using the program on a machine without sound capability. That setting is on the same sub menu where heuristics may be deactivated, and also the choice made to scan every byte in each file, rather than the parts more usually scanned by 'top-and-tailing' and entry point tracing and emulation.

On-access Scanner

The setup utility for the on-access scanner presents much the same options and screen layout as the configuration menu for the on-demand scanner, except that it replaces the location to scan settings with an on/off toggle. Although the other tab pages have the same names, most present rather fewer choices than their counterparts. The choice of actions upon detection of an infected object is disinfection, denial of access and automatic deletion of the file. Options depend on heuristics and warnings being 'on' or 'off'. Somewhat disturbingly, the on-access scanner was prone to producing fatal errors on one of the test machines. The program also fails to check for disks in the A: drive at shutdown, allowing the potential to boot from an infected floppy.

Scanning and Detection

The shortcomings in *AVP's* documentation can be forgiven if the anti-virus engine performs well enough. The interface for the on-demand scanner is simple and well-planned, with options easily reached from a single selection of tabbed menus. The standard scanning method, as for the on-demand scanner, checks a pre-selected set of file types as well as applying heuristics. Available configuration options allow heuristics to be 'off' or 'on', a choice of extensions to be scanned, and the introduction of 'redundant' scanning.

This final type of scan checks every byte of code, rather than the most likely infection sites at the start and end of the scanned files. When selecting this option, you are warned that the scan will take longer, and may result in false alarms. In testing, the setting made no difference whatsoever, apart from increasing scan times.

Overall, the detection rate was very impressive. All In the Wild boot and file, polymorphic and standard virus samples were detected by a standard scan. Identical detection results were also achieved using the standard settings for the on-access scanner.

The only misses in the whole test were the four samples of the relatively new macro virus W97M/AntiSR1.A, which was for some time considered impossible to replicate and thus merely an intended virus. Given *AVP's* otherwise impeccable record, it seems likely that *Kaspersky Lab* was under this misapprehension when the tested release was produced. Of the viruses detected, all four samples of a single macro virus (WM/MortalKombat) were flagged as suspicious by *AVP's* heuristics, and one sample of an ItW virus was shown as a possible new variant of itself. In all other cases, an exact name was provided for the virus.

Not surprisingly, the virus detected using heuristics was missed with this facility switched 'off', but the other results remained identical. The Clean test-set does double-duty, serving as the basis of our timing and overhead tests (see below), and as a false-positive test. In the latter, *AVP's* performance proved less satisfactory. It produced six false positives, all as a result of over-keen heuristics rather than poorly chosen virus patterns.

Time Trials

The speed at which *AVP* produces these commendable results is a significant factor. The standard for judging speed of on-demand scanning is the Clean test-set, and this was scanned with heuristics 'on' and 'off', and redundant scanning 'on' and 'off'.

With its default settings, *AVP* scanned the Clean test-set in 57.5 seconds, or a scanning rate of 0.9 MB/s, and produced six false positive reports. Turning heuristic scanning off resulted in a scanning time of 52.5 seconds – a data rate of 1.0 MB/s – and removed the false positives. Enabling redundant scanning and heuristics then repeating the test took 4210 seconds at a data rate of 130 KB/s, and brought back the false positives. Finally, disabling heuristics again removed the false positives and slightly reduced the scanning time to 4255 seconds.

Obviously, the warning about the extra overhead of the redundant scan should not be taken lightly! The effect of the heuristic monitor is all but negligible in comparison with the basic time penalty for the pattern-checking part of the program. The speed of its decision-making capabilities regarding infection were tested in comparison to floppy disk scans. The disks had identical contents, except that on one diskette all the program files were infected with Natas.4744. Using *AVP's* default on-demand scanning settings, the clean diskette was inspected in 53 seconds, while the infected disk took 42 seconds to check.

As users come to rely more on resident or on-access scanners, the performance overhead of these components becomes increasingly important. The overhead of *AVP's Monitor* was measured using the same method used in the *Windows 95* comparative in this issue (see p.10). Enabling the on-access scanner resulted in an overhead of 18%. The default on-access setting has heuristics disabled – enabling heuristics and rerunning the test resulted in an additional 8% overhead. This level of overhead will likely prove a little tedious, but again heuristics are not the dominating factor in the slowdown.

Conclusion

With an all but perfect detection rate *AVP* certainly does the job it sets out to, with any problems encountered more cosmetic than functional. The manual remains the most obvious offender, being not only obsolete but in some cases misleading. On the other hand, if the quality of on-line help in the on-demand scanner is anything to go by, the matter can clearly be corrected.

AVP's design lends itself to easy understanding. It is more pleasant to use than some products that boast great reference tomes in perfect English – ultimately, detection rates are more important. On this front all is well, but as ever improvements could be made. Overhead and scanning times are still on the sluggish side, and any false positives are too many. Overall, a fine product, the quality of scanning throwing into sharp relief its few faults.

Technical Details

Product: *AVP for Windows 95.*

Developer: *Kaspersky Lab*, 10 Geroev Panfilovtcev str, 123363 Moscow, Russia, Tel +7 095 9484331, fax +7 095 9135087, email sales@avp.ru, WWW http://www.avp.ru/.

Vendors: UK – NEST Ltd, 53 Gunhild Way, Cambridge, CB1 4QZ, Tel +44 1223 565058, fax +44 1223 565058, email avp-support@nest.compulink.co.uk; USA – Central Command Inc, PO Box 856, Brunswick, OH 44212, Tel +1 330 2732820, fax +1 330 2204129, sales@command-hq.com, WWW http://www.command-hq.com/command/.

Availability: This program requires 4 MB of memory and 2.5 MB of free disk space.

Version Evaluated: Version 3.0, build 119.

Price: Single user licence with one year's update subscription, $68. There are various discounts for extending licences beyond a single year, for site licences and for use in educational and government settings – contact a vendor for details.

Hardware Used: 166 MHz Pentium-MMX workstations with 64 MB RAM, 4 GB hard disk, CD-ROM drive and 3.5-inch floppy drive running *Windows 95 (SP1)*. 233 MHz AMD K6 workstation with 48 MB RAM, 1.6 GB hard disk, 2 CD-ROM drives and 3.5-inch floppy drive.running *Windows 95*.

Test-sets: Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/Win95/199805/test_sets.html.

SUBSCRIPTION RATES

Subscription price for 1 year (12 issues) including first-class/airmail delivery:

UK £195, Europe £225, International £245 (US$395)

Editorial enquiries, subscription enquiries, orders and payments:

Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP, England

Tel 01235 555139, International Tel +44 1235 555139
Fax 01235 531889, International Fax +44 1235 531889
Email: editorial@virusbtn.com
World Wide Web: http://www.virusbtn.com/

US subscriptions only:

Virus Bulletin, 18 Commerce Way, Woburn, MA 01801, USA

Tel (781) 9377768, Fax (781) 9320251

END NOTES AND NEWS

Infosecurity Asia 1998 will take place at the Singapore International Convention and Exhibition Centre from 25–27 June 1998. The event includes anti-virus issues in its corporate IT security programme. Contact Karen Binwani or Rose Zama at *Reed Exhibitions Pte Ltd* in Singapore for details; Tel +65 434 3663/3698.

NetSec '98: Network Security in the Open Environment will focus on the security issues, problems and solutions facing networked environments. The conference is to be held at the **Hyatt Regency Hotel in San Antonio, Texas from 15–17 June 1998**. Contact *CSI* for further details; Tel +1 415 9052626, fax +1 415 9052218, email csi@mfi.com, or visit the web page at http://www.gocsi.com/.

***Integralis Technology Ltd* is now trading under the new name of *Content Technologies Ltd*.** The organization's head office in the United Kingdom has moved to Forum 1, Station Road, Theale, Berkshire, RG7 4RA; Tel +44 118 9301300, fax +44 118 9301301, visit the company's Web site http://www.mimesweeper.com or email info@mimesweeper.com for more information.

The Computer Evidence and Investigations Unit at *Network International* is hosting a one-day training course at the Millenium Britannia Mayfair Hotel in London. 'Investigating Computer Crime and Misuse' will take place on Wednesday 3 June 1998. To register for a place on the course contact Catrin Jones at *Network International*; Tel +44 171 3448100, fax +44 171 3448161, or email cjones@nsml.com.

Data Fellows* and the Swedish company *TenFour* have agreed to a cooperation deal which bundles *TenFour's TFS Gateway* with *Data Fellows' F-Secure Anti-Virus (FSAV). The result is a 'uniquely comprehensive mail gateway product' according to Teemu Lehtonen, Product Manager for *FSAV*. Contact Mr Lehtonen at *Data Fellows'* head office in Finland for further details; Tel +358 9 859900, fax +358 9 85990599, email Teemu.Lehtonen@DataFellows.com, or visit the company's Web site http://www.DataFellows.com/.

***Sophos* is hosting a practical *NetWare* security course** at its training suite in Abingdon, UK on **Thursday 9 July 1998**. For details, contact Karen Richardson; Tel +44 1235 544015, fax +44 1235 559935 or visit the company's Web site; http://www.sophos.com/.

Compsec '98, the fifteenth World Conference on Computer Security, Audit and Control will take place from **11–13 November 1998, at the Queen Elizabeth II Conference Centre in London, UK.** The agenda includes an exhibition, a pre-conference workshop on 10 November and the Seventh Annual Directors' Briefing on 13 November. Early bird discounts are available for registrations received before 15 May. For details and a registration form, contact the conference secretary Amy Richardson; Tel +44 1865 843643, fax +44 1865 843958, email a.richardson@elsevier.co.uk, or visit the new Compsec '98 Web site http://www.elsevier.nl/locate/compsec98/.

***Dr Solomon's Software* is running two-day live virus workshops at Barnes Hotel, Bedford, UK from 12–13 May and 16–17 June 1998.** The course costs £695 + VAT. Contact Caroline Jordan for details; Tel +44 1296 318881 or email Caroline.Jordan@drsolomon.com.

Portcullis Computer Security Ltd announces the release of ***Portcullis' Enterprise Network Security* (*PENS*) for all 32-bit *Windows* systems.** Comprised of six modules, *PENS'* anti-virus component is based on the combination of *F-PROT* and *AVP* engines used by *Data Fellows*. Further information is available from Technical Director, Paul Docherty; Tel +44 181 8680098, fax +44 181 8680017, or email pjd@portcullis-security.com.

Following the appearance of Access97M/AccessiV (as featured in last month's issue, p.15), **American software consulting firm FMS announced the release of FMS Access Virus Scanner.** The utility is available free from the company's Web site http://www.fmsinc.com/.

GartnerGroup presents the Information Security Conference 1998 from 18–19 June 1998 at the Royal Lancaster Hotel, London, UK. For more information about the conference agenda and registration details; Fax +44 1784 488987 or email ppearce@gartner.com.

Network managers and administrators can install and manage anti-virus software centrally with the new release of ***Dr Solomon's Management Edition v1.50***. The product covers *Windows 3.1*, *Windows for Workgroups 3.11*, *Windows 95*, *NT* and *Novell NetWare* platforms. All of these platforms can be updated from a central location. Contact Rosemary Barnes; Tel +44 1296 318700 or email rosemary.barnes@uk.drsolomon.com for availability.